EXHIBIT 6

Filed on behalf of Unified Patents Inc.
By: Jason R. Mudd, Reg. No. 57,700
Eric A. Buresh, Reg. No. 50,394
ERISE IP, P.A.
6201 College Blvd., Suite 300
Overland Park, KS 66211
Tel: (913) 777-5600
Email: jason.mudd@eriseip.com

Jonathan Stroud, Reg. No. 72,518
UNIFIED PATENTS INC.
1875 Connecticut Ave. NW, Floor 10
Washington, D.C., 20009
Tel: (202) 805-8931
Email: jonathan@unifiedpatents.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.
Petitioner

v.

TEXTILE COMPUTER SYSTEMS, INC.
Patent Owner

IPR2017-00296
Patent 8,505,079

PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,505,079

TABLE OF CONTENTS

I. INTRODUCTION

Petitioner Unified Patents Inc. ("Petitioner") respectfully requests an *Inter Partes* Review ("IPR") of claims 1, 3, 6–9, 11, 13, and 16–19 (collectively, the "Challenged Claims") of U.S. Patent 8,505,079 ("the '079 Patent"). Despite dating back to just 2011, the '079 Patent purports to have invented and broadly claims a system and method for authenticating a request by an authorized user (e.g., purchaser) for an unauthorized service client (e.g., merchant) to be given limited access to a secured resource (e.g., payment account) using a standard three-party tokenization protocol. The '079 Patent faced just one rejection over a single prior art reference during prosecution.

But, as demonstrated below, the claimed three-party protocol, which uses "dummy" key strings (or tokens) rather than sensitive account numbers "in-the-clear," was both well known and obvious many years prior to 2011. Petitioner submits the expert declaration of Stephen Mott, a 30-year industry veteran in the field of electronic payment systems and security, in support of this petition. *See Mott Decl.* (EX1007). As explained by Mr. Mott, payment tokenization technologies that use tokens generated by a third-party payment provider, rather than transmitting sensitive account numbers "in-the-clear" to merchants, were well known by October 2011 and had been developed over a decade earlier. *See id*. at ¶¶28-58.

II. SUMMARY OF THE '079 PATENT

A. Description of the alleged invention of the '079 patent

The '079 Patent relates to authentication. It describes a basic three-party transaction protocol "whereby the identity of a person, entity, device or the like attempting to gain access to a secured resource may be securely authenticated." *'079 Patent* (EX1001), at Abstract. In particular, the disclosed protocol enables an end-user to request access to a secure resource, such as a bank account, for an unauthorized service client, such as a retailer, without revealing confidential information (e.g., the end-user's bank account number) to the unauthorized service client. *Id.* at 7:47-8:10, 10:9-36.

The protocol, which is illustrated in the annotated version of Figure 4 below, uses six (6) basic messaging steps between an end-user 34 (e.g., consumer/purchaser), a service client 33 (e.g., retailer/merchant), and a service provider 36 (e.g., financial institution/payment provider):

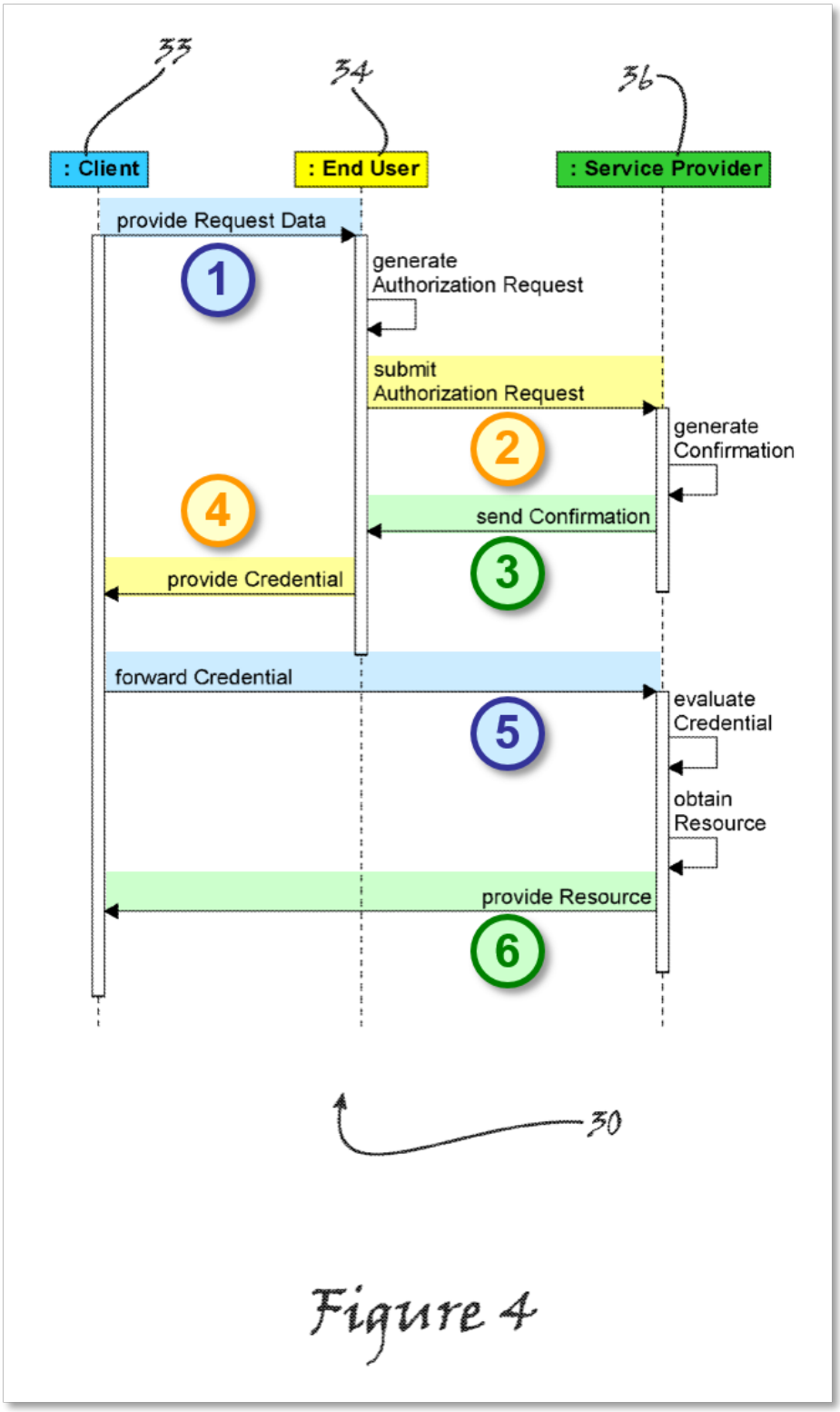
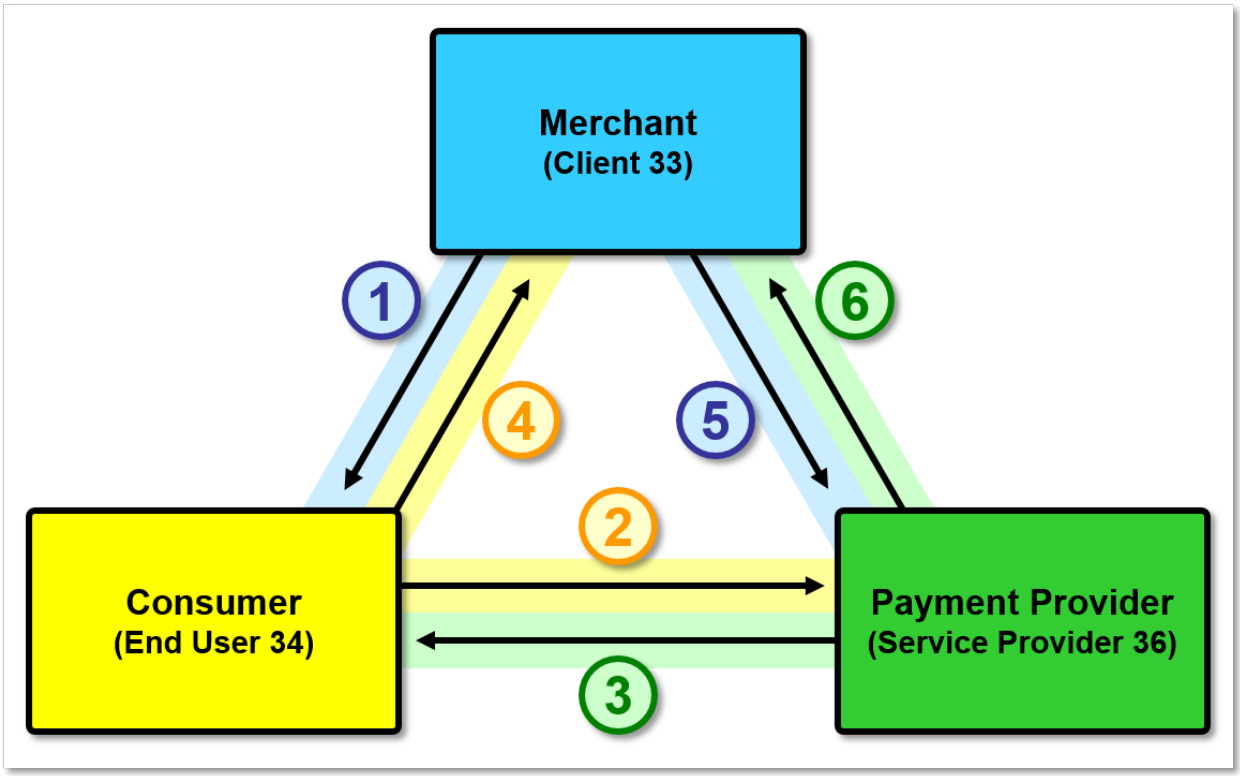


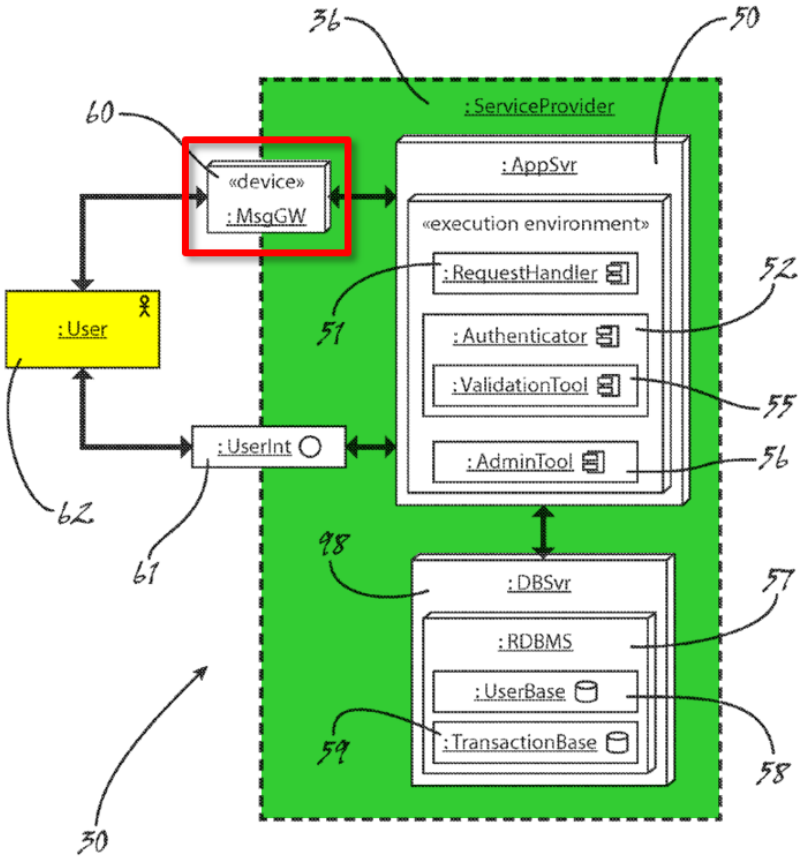
Figure 4

Id. at Fig. 4; *see also, id.* at 5:35-7:13, 8:47-52, 10:9-28.

For clarity, the process can also be illustrated like so:



In step 1, to initiate the transaction, the service client 33 sends request information to the end user 34. *Id.* at 5:35-40, 10:37-42. The request information may include a service client's identifier and a purchase amount. *Id.* at 5:40-45, 10:42-44, 10:66-11:4, Fig. 9. In step 2, the end-user 34 uses the request information to generate a request message, which is then sent from the end-user 34 to the service provider 36. *Id.* at 5:45-49, 11:48-52. The request message may be sent via text message, e-mail, voice, or over a web interface. *Id.* at 9:35-50, 11:54-12:9. In one embodiment, the request message is received by a messaging gateway 60 (denoted in the Figure below), which receives the request message from the end-user and forwards it to a service provider server 50:



Id. at Fig. 5 (annotated); *see also, id.* at 13:34-38.

The service provider 36 receives the request message and determines whether or not the end-user 34 is authorized to use the system. *Id.* at 5:50-60, 13:39-46. If the end-user 34 is authorized, the service provider 36 determines the identity of the resource to which access is to be granted (e.g., the end-user's checking account) and creates a transaction record storing the end user's information, the service client identifier, a resource identifier, and other pertinent information such as the purchase amount. *Id.* at 5:60-6:11; 13:46-57. At the same time, the service provider 36 determines "the appropriate key string for use in positively authenticating the identity of the presently tentatively identified end user

34" and stores it in the transaction record. *Id.* at 14:66-15:21.

In step 3, the service provider 36 then generates a confirmation message 94 and sends it to the end-user 34. *Id.* at 6:12-18, 15:42-56. Once the end-user receives the confirmation message 94, he or she will submit an authentication credential to the service client 33 in step 4. *Id.* at 6:18-21, 15:57-16:15. The "authentication credential simply comprises a previously established key string known to both the service provider 36 and the end user 34." *Id.* at 6:26-28. After receiving the end-user's authorization credential, the service client 33 forwards it to the service provider 36 for validation in step 5. *Id.* at 6:28-32, 16:16-35. The service provider 36 validates the authorization credential "by comparing the credential against a known key string . . . the known correct key string will simply be the same key string known to both the service provider 36 and the end user 34." *Id.* at 6:45-55. If the authorization credential is valid, the service provider 36 provides the service client 33 access to the requested secure resource in step 6. *Id.* at 7:4-13, 16:35-40.

B. Summary of the prosecution history of the '079 patent

The U.S. Patent Application that resulted in the '079 Patent was filed on October 23, 2011. *'079 Patent File History* (EX1002), at 182. For purposes of this proceeding, Petitioner is assuming that the priority date for the Challenged Claims is October 23, 2011. The original application included 20 claims. *Id.* at

219–224. Notably, as-filed claims 1-8 included many limitations written in means-plus-function format. *Id.* at 219–221. On January 2, 2013, the USPTO issued an Office Action rejecting claims 1-8 as being indefinite under §112, ¶2 for including means-plus-function limitations not clearly linked to specific structures in the specification. *Id.* at 105–109. Additionally, all 20 original claims were found to be anticipated under §102(b) by U.S. Patent Publication 2009/0259588 to Lindsay ("*Lindsay*"). *Id.* at 109–117.

Of relevance, *Lindsay* discloses a security system for protecting access to an asset such as a credit account. *Lindsay* (EX1003), at Abstract, [0064]. When a user attempts to pay a merchant using the system, the user provides his or her credentials to the merchant. *Id.* at [0198]. The credentials include a password and a user ID or account number. *Id.* at [0020]. The password may be a primary or secondary password. *Id.* at [0198]. The secondary password provides limited access to the protected asset. *Id.* at [0087]. The merchant sends the user's credentials to a credit card company, which validates the transaction by "compar[ing] the user info and credentials with information stored in the credit database . . . ." *Id.* at [0199].

On April 2, 2013, Applicant filed an amendment removing the means-plus-function limitations from claims 1-8 and amending independent claims 1 and 11 to distinguish over *Lindsay*. *'079 Patent File History* (EX1002), at 72-82. The

amendments to claim 1 are depicted below:

> 1. (currently amended) An authentication system for authenticating the identity of a requester of access by an unauthorized service client ~~user~~ to a secured resource, said authentication system comprising:
>
> a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to ~~means for~~ receive[[ing]] from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized ~~user~~ service client to said secured resource;
>
> a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to ~~means for~~ determine[[ing]] a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester;
>
> a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client;
>
> wherein said second set of instructions is further operable to ~~means for~~ receive[[ing]] an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requestor; and
>
> wherein said second set of instructions is further operable to ~~means for~~ evaluate[[ing]] said authentication credential to authenticate the identity of said requester.

Id. at 73.

Applicant argued that *Lindsay* does not anticipate because "Lindsay discloses an *authorized* service client, which is the merchant (828) shown in Fig.

17. Lindsay *does not* teach providing a resource to an *unauthorized* service client, which is the thrust of Applicant's invention." *Id.* at 80–81 (emphasis in original). While Applicant did not explain why he felt *Lindsay's* merchant is an "authorized" service client, a reasonable inference is that it is because *Lindsay* discloses that the credentials provided to the merchant may include the user's account number. *Lindsay* (EX1003), at Fig. 17, [0020], [0059], [0198]. The '079 patent specification states that a "critical aspect" of the invention is that the service client never be given access to "the common identifier for the secured resource, e.g. the account number for a credit card or financial deposit account; the Social Security Number of a patient; the account number of an ATM card; or the like." *'079 Patent* (EX1001), at 8:4-10. That, of course, is the purpose for the '079 Patent using a three-party tokenization architecture.

Applicant also argued that *Lindsay* does not disclose "receiving an authorization request from an end user for access by an unauthorized service client to the secured resource, as recited in Claim 1 and Claim 11" because "Lindsay does not even teach the end user communicating any part of the transaction with the service provider." *'079 Patent File History* (EX1002), at 81–82.

The USPTO issued a notice of allowance on June 6, 2013 stating that the Applicant's arguments were persuasive and including an examiner's amendment incorporating limitations from claim 1 into independent claim 11. *Id.* at 21–31.

The '079 Patent issued on August 6, 2013. *'079 Patent* (EX1001).

III. REQUIREMENTS FOR INTER PARTES REVIEW UNDER 37 C.F.R. § 42.104

A. Grounds for standing under 37 C.F.R. § 42.104(a)

Petitioner certifies that the '079 patent is available for IPR and that the Petitioner is not barred or estopped from requesting IPR challenging the claims of the '079 patent.

B. Identification of challenge under 37 C.F.R. § 42.104(b) and relief requested

In view of the prior art and evidence, claims 1, 3, 6–9, 11, 13, and 16–19 of the '079 patent are unpatentable and should be cancelled. 37 C.F.R. § 42.104(b)(1). Based on the prior art references identified below, IPR of the Challenged Claims should be granted. 37 C.F.R. § 42.104(b)(2).

Proposed Grounds of Unpatentability	Exhibit Nos.
Ground 1: Claims 1, 6, 7, 9, 11, 16, 17, and 19 are **obvious** under § 103(a) over U.S. Patent Application Publication No. 2006/0235796 to Johnson et al. ("*Johnson*") in view of U.S. Patent No. 7,657,489 to Stambaugh ("*Stambaugh*")	EX1004 and EX1005
Ground 2: Claims 1, 3, 6–9, 11, 13, and 16–19 are **obvious** under § 103(a) over *Johnson* in view of *Stambaugh* in further view of U.S. Patent Application Publication No. 2006/0173794 to Sellars et al. ("*Sellars*")	EX1004, EX1005, and EX1006

Section IV identifies where each element of the Challenged Claims is found

in the prior art patents. 37 C.F.R. § 42.104(b)(4). The exhibit numbers of the supporting evidence relied upon to support the challenges are provided above and the relevance of the evidence to the challenges raised are provided in Section IV. 37 C.F.R. § 42.104(b)(5). **Exhibits EX1001 – EX1016** are also attached.

C. Level of skill of a person having ordinary skill in the art

As explained by Mr. Mott, the use of payment tokenization technologies in the electronic payments industry (*e.g.*, using "tokens" or "virtual accounts" rather than account credentials "in-the-clear") dates back over a decade prior to 2011. *Mott Decl.* (EX1007), at ¶¶28-58. While merchant point-of-sale (POS) systems had traditionally relied on two-factor authentication through requiring the consumer's card (i.e., something the consumer has) and PIN (i.e., something the consumer knows), the advent of the Internet and eCommerce created the need for new solutions. *Id.* at ¶¶30-34. Because encryption alone proved problematic, by about the year 2000 many companies like Amazon.com, Cardinal Commerce, American Express, eBay, PayPal, Microsoft, and RSA Security began using three-party tokenization solutions that replaced sensitive account numbers with tokens or virtual account numbers. *Id.* at ¶¶35-43. Many patents using three-party tokenization protocols very similar to the '079 patent had been filed in this same time frame, more than a decade prior to the '079 patent. *See, e.g.,* EX1015 (*Franklin*), EX1016 (*Wronski*), EX1009 (*Bhagavatula*), EX1010 (*Keresman*).

By 2005, MasterCard had developed a "Virtual Debit Card" using a unique, one-time-password (OTP) token submission for payment and was similar to the OTP offerings of companies like Cyota and Orbiscom at the time. *Id*. at ¶¶47-49. Also by 2005, FFIEC had issued guidelines calling for second factor authentication by banks and suggested payment tokens as one such available technology. *Id*. at ¶50. By August 2011, substantial industry acceptance and deployment had already occurred—with billions of tokens having already been issued—and, in fact, the Payment Card Industry Council (PCI) had already published industry guidelines for tokenization. *Id*. at ¶¶46, 52-54.

Payment tokenization for mobile devices was also already being deployed in the industry on a large scale by May 2011, with Google's mobile "wallet." *Id*. at ¶¶55-57. Indeed, payment tokenization using mobile devices had already been known and disclosed many years before, as demonstrated by *Johnson* and *Stambaugh*, which are discussed in detail in Section IV.A below; and, as discussed, *Johnson* discloses the same basic 6-step three-party tokenization protocol as the '079 patent. *See* Sec. IV.A, *infra*. It is difficult to conceive how the broad claims of the '079 patent were thought to be knew and non-obvious as of October 2011. *Mott Decl.* (EX1007), at ¶58.

A person having ordinary skill in the art at the time of the '079 patent would have been a person having the equivalent of either a business degree (e.g., a

bachelor's in business, economics, finance or similar discipline) or a degree in computing (e.g., a bachelor's in computer science, electrical engineering, or similar discipline), with sufficient practical experience (i.e., at least two years) in designing and deploying electronic payment and security systems. *Id.* at ¶60.

D. Claim construction under 37 C.F.R. § 42.104(b)(3)

In this proceeding, claim terms of an unexpired patent should be given their "broadest reasonable construction in light of the specification." 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144-46 (2016). Petitioner proposes the below specific constructions, and all claim terms not specifically discussed below should be given their broadest reasonable construction in light of the specification.

i. Unauthorized service client

Claims 1 and 11 recite a system and method for requesting "unauthorized service client" access to a secured resource. *'079 Patent* (EX1001), at 17:28-30, 18:42-45. Regarding service client access to secured resources, the '079 patent specification discloses:

> With the foregoing broad overview of the general structure and function of the authentication system 30 of the present invention in mind, it is now noted that in accordance with the present invention an end user 34 may comprise any person or machine requiring, in connection with some other use, access or other relationship with a service client 33, access for the service

> client 33 to a secured resource **for which the service client 33 is restricted from full knowledge** and for which the service provider 36 may hold full knowledge, **full knowledge being defined herein as knowledge sufficient to make ordinary full use of the secured resource outside of the framework of the authentication system 30 and method 46** of the present invention.

Id. at 7:14-26 (emphasis added). As an example of such a restriction, the '079 patent discloses restricting service client access to the common identifier of the secured resource, such as "the account number for a credit card or financial deposit account" and the like. *Id.* at 8:4-10 (emphasis added).

Therefore, the broadest reasonable interpretation of "unauthorized service client" should at least include "a service client that is restricted from knowledge sufficient to make ordinary full use of the secured resource outside of the framework of the authentication system."

ii. Messaging gateway

Claim 1 recites "a messaging gateway . . . operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource." *Id.* at 17:31-36. Claim 11 recites a similar "messaging gateway" limitation. *Id.* at 18:38-45. Regarding a "messaging gateway," the '079 patent discloses "a preferably unified messaging gateway 60" that facilitates communication of messages between the

end user 34 and service provider 36 using "**a plurality of message formats** (such as, for example, as a short messaging service ("SMS") message, a standard text message, an e-mail message, a synthesized voice message, an alphanumeric page or the like) **over any of a plurality of communication channels** (such as, for example, an SMS or other text channel, a simple mail transport protocol ("SMTP") channel, a plain old telephone system ("POTS") channel, a paging network or private broadcast channel or the like) to be received by any of a plurality of user devices (such as, for example, a mobile or landline telephone, a smart phone, an e-mail client, a personal data assistant ("PDA"), a numeric or digital pager or the like)." *Id.* at 9:32-50 (emphasis added); *see also id*. at 11:54-62, 12:20-49.

In claims 1 and 11, the only recited functions of the claimed messaging gateway is to receive the request for access from the authorized user (e.g., end user) and to be in secure communication with the server (e.g., server of the service provider, such as a financial institution). *Id*. at claims 1 & 11. Additionally, messaging gateways were well known in the art, including in secured payment systems, prior to the '079 Patent, as being devices that can transfer information between networks that use different communications protocols (e.g., different message formats) by converting the information into a form compatible with the protocol used by the receiving network (e.g., by converting the message format). *Mott Decl.* (EX1007), at ¶68; *Microsoft Computer Dictionary* (EX1014)

("gateway").

Therefore, the broadest reasonable interpretation of "messaging gateway" should at least include "a device for use in transferring messages between a plurality of communications channels by converting messages between a plurality of message formats."

iii. Key string

Claims 1 and 11 recite, "a key string known to both said secured resource and the authorized user . . . said key string being adapted to provide a basis for authenticating the identity of said requester." *'079 Patent* (EX1001), at 17:40-43, 18:46-53. Based on the '079 patent's express definition of the term "string," the broadest reasonable interpretation of "key string" should at least include "an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user 34 and a format that may be recognized by software or hardware that may be used to provide a basis for authenticating the identity of the requester." *Id.* at 15:29-36.

IV. THERE IS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS OF THE '079 PATENT ARE UNPATENTABLE

A. Ground 1: *Johnson* in view of *Stambaugh* renders claims 1, 6, 7, 9, 11, 16, 17, and 19 obvious

U.S. Patent Application Publication 2006/0235796 to Johnson et al. ("*Johnson*") was published on October 19, 2006 and therefore qualifies as prior art with regard to the '079 patent under 35 U.S.C. § 102(b) (pre-AIA). *Johnson* (EX1004). *Johnson* was not cited during prosecution of the '079 patent. *See '079 Patent* (EX1001). *Johnson* teaches "authorization and payment of an online commercial transaction between a purchaser and a merchant including verification of an identity of the purchaser." *Johnson* (EX1004), at Abstract. *Johnson* also teaches the alleged "critical aspect" of the '079 patent invention in that a merchant is never granted access to the purchaser's account information. *Id.* at [0014], [0042], [0067].

Johnson discloses the exact three-party transaction protocol identified by Applicants as a patentable feature of their invention. In particular, *Johnson* teaches a system including a client/purchaser 110, which is the same as the '079 patent's end-user 34 (denoted in yellow below); a service provider/merchant 140, which is the same as the '079 patent's client 33 (denoted in blue below); and the payment provider 130, which is the same as the '079 patent's server provider 36 (denoted in

green below). As also denoted in the figures below, the protocols disclosed by the '079 patent and *Johnson* each comprise the same six steps including:

(1) the service client/merchant provides request information to the end-user/purchaser;

(2) the end-user/purchaser sends a request to the service provider/payment provider;

(3) the service provider/payment provider sends a confirmation/token back to the end-user/purchaser;

(4) the end-user/purchaser provides an authorization credential/payment token to the service client/merchant;

(5) the service client/merchant forwards the authorization credential/payment token to the service provider/payment provider; and

(6) the service provider/payment provider validates the authorization credential/payment token and completes the transaction.

Johnson

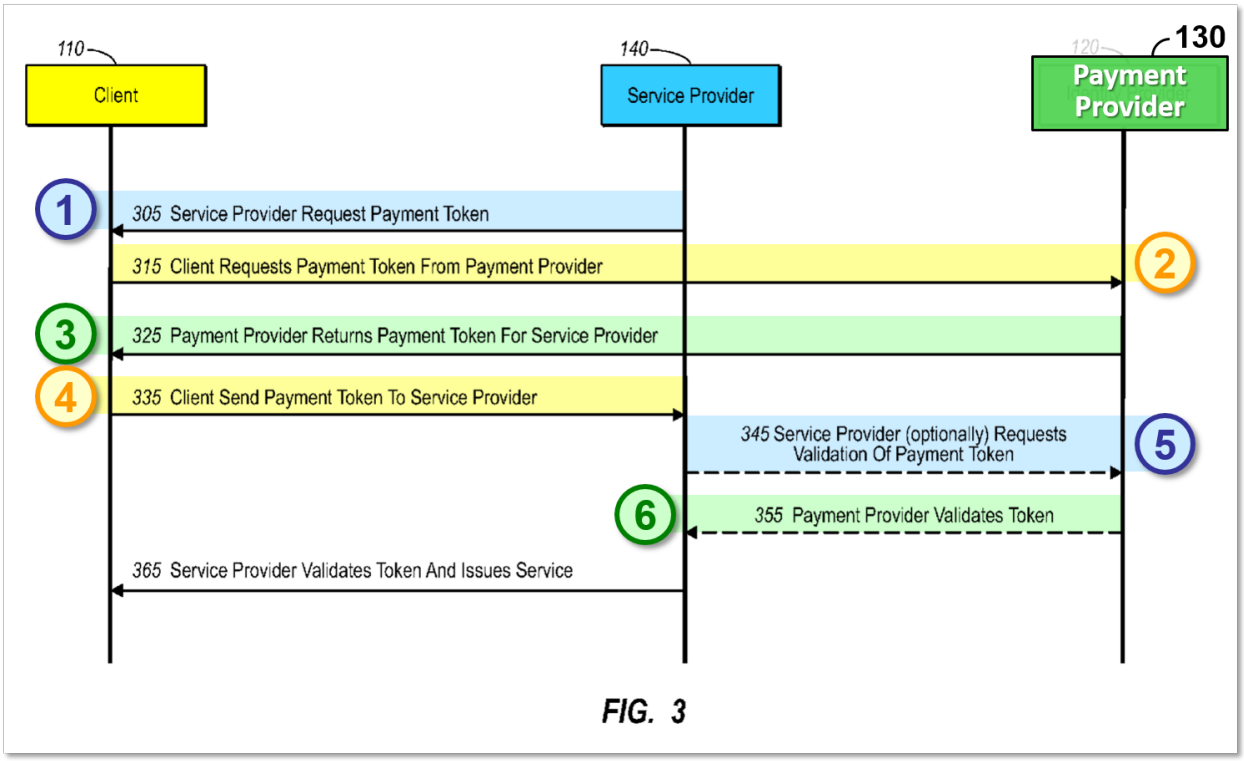


FIG. 3

Id. at Fig. 3 (annotated).[1]

[1] Petitioner notes that Figure 3 of *Johnson* has a typographical error. The box labeled as "Identity Provider 120" should be "Payment Provider 130," as is clear from the specification. *Johnson* (EX1004), at [0059]. A PHOSITA would understand the same. *Mott Decl.* (EX1007), at ¶63. Petitioner's annotation to Figure 3 makes this correction.

'079 Patent

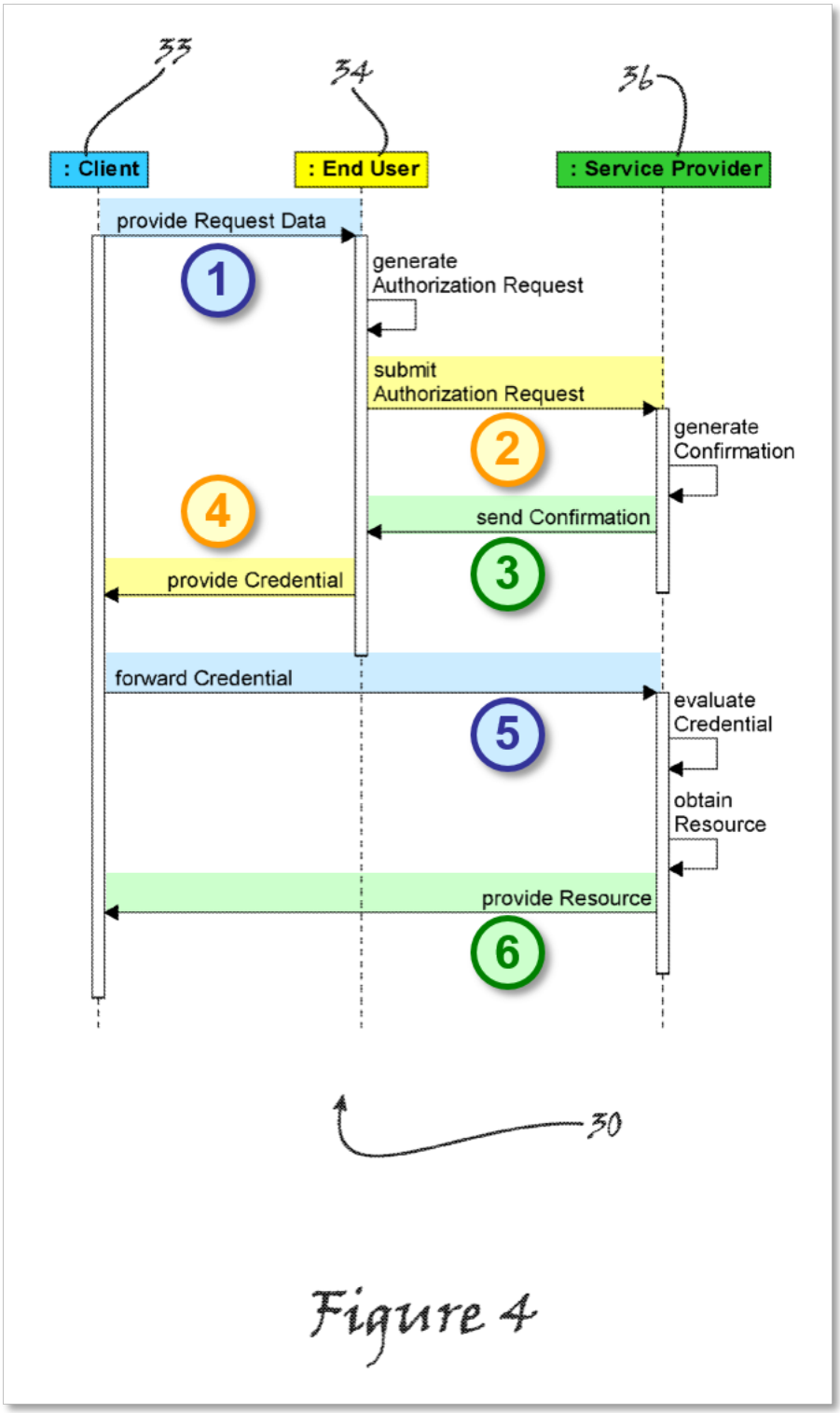


Figure 4

'079 Patent (EX1001), at Fig. 4 (annotated).

The '079 patent relates to "security protocols for use in securing and/or restricting access to personal other [sic] confidential information, physical locations and the like" and a system and method "whereby the identity of a person, entity, device or the like attempting to gain access to a secured resource may be securely authenticated." *Id.* at 1:6-12. For reasons described above, *Johnson* also relates to a security protocol for securing and/or restricting access to personal or other confidential information. *Johnson* (EX1004), at [0010], [0013]–[0014], [0032]–[0038]. *Johnson* also teaches securely authenticating the identity of the end-user attempting to gain access to financial accounts held by a payment provider. *Id.* at Abstract, [0033], [0042]. As such, *Johnson* is in the same field of endeavor and is analogous to the claimed invention of the '079 patent. *See also Mott Decl.* (EX1007), at ¶¶64-66.

The '079 patent seeks to solve problems associated with "the age old process of providing a privately held password, personal identification number or the like in attempting to gain access to the secured resource." *'079 Patent* (EX1001), at 1:29-34. In particular, '079 patent seeks to prevent interception of this sensitive information by an attacker. *Id.* at 1:34-38. *Johnson* also aims to prevent "security breaches resulting in loss of personal, financial and/or other confidential information." *Johnson* (EX1004), at [0010]; *see also, id.* at [0003]. Therefore, *Johnson* is reasonably pertinent to the problem faced by the inventor of the '079

patent and is therefore analogous to the claimed invention of the '079 patent. *See also Mott Decl.* (EX1007), at ¶¶64-66.

U.S. Patent 7,657,489 to Stambaugh ("*Stambaugh*") issued on February 2, 2010 and therefore qualifies as prior art with regard to the '079 patent under 35 U.S.C. § 102(b) (pre-AIA). *See Stambaugh* (EX1005). *Stambaugh* also teaches a three-party transaction protocol authenticating the identity of a user requesting merchant access to funds in a protected account. *Id.* at 2:18-50. When a user wishes to purchase an item from a merchant, the user's mobile device is used to transmit the user's PIN to a payment authority via text message, e-mail or voice message. *Id.* at 2:23-27, 3:53-65, 6:25-31, 6:51-56. The message also includes the user's mobile identification number, which is used by the payment authority in combination with the PIN to authenticate the user. *Id.* at 6:31-33. If the user is authenticated, the payment authority generates a transaction code, which is then sent back to the user. *Id.* at 7:11-26, 8:19-30. Once the user receives the transaction code, he or she may append an additional code to the received transaction code. *Id.* at 8:19-30. The digits of the code appended to the transaction code by the user are known only to the payment authority and the user and are used to provide an additional factor of authentication as to the identity of the user. *Id.* The user provides the augmented transaction code to the merchant, which submits it to the payment authority via a transaction authority. *Id.* at 7:26-44. The

payment authority evaluates the received transaction code and recognizes it as valid if the code includes the digits originally generated by the payment authority in addition to the digits of the code known only to the user and the payment authority. *Id.* at 7:44-46, 8:19-30. After approving the transaction, the payment authority "can instruct that the appropriate funds be sent to the respective merchant's bank accounts." *Id.* at 7:59-61.

As discussed above, the '079 patent relates to "security protocols for use in securing and/or restricting access to personal other [sic] confidential information, physical locations and the like" and a system and method "whereby the identity of a person, entity, device or the like attempting to gain access to a secured resource may be securely authenticated." *'079 Patent* (EX1001), at 1:6-12. As described above, *Stambaugh* teaches a security protocol that authenticates the identity of a user attempting to access an account. *Stambaugh* (EX1005), at 2:18-50, 2:61-3:5. *Stambaugh* is in the same field of endeavor and is therefore analogous to the claimed invention of the '079 patent. *See also Mott Decl.* (EX1007), at ¶¶69-70.

The '079 Patent also seeks to "provid[e] a system and related method by which authentication may be more securely conducted . . . [that] is robust in specific implementation and readily usably by any manner of person, entity, device or the like." *'079 Patent* (EX1001), at 1:45-53. *Stambaugh* similarly seeks to provide a wireless payment transaction system utilizing a multifactor

authentication in an effort to "virtually eliminate fraudulent transactions" while still maintaining convenience and speed. *Stambaugh* (EX1005), at 1:13-16, 1:54-64, 2:4-14. Therefore, *Stambaugh* is reasonably pertinent to the problem faced by the inventor of the '079 patent and is therefore analogous to the claimed invention of the '079 patent. *See also Mott Decl.* (EX1007), at ¶¶69-70.

i. Claim 1

1. An authentication system for authenticating the identity of a requester of access by an unauthorized service client to a secured resource, said authentication system comprising:

Johnson teaches a system providing "authorization and payment of an online commercial transaction between a purchaser and a merchant including **verification of an identity** of the purchaser and verification of an ability of the purchaser to pay for the transaction." *Johnson* (EX1004), at Abstract (emphasis added). In particular, *Johnson's* system authenticates the identity of a purchaser/consumer (i.e., "requester") for purposes of granting a merchant (i.e., "unauthorized service client") access to funds in the purchaser's billing account (i.e., "secured resource"). In one embodiment, the purchaser's identity is authenticated using a payment token:

> Further, because the merchant can validate the payment token directly with the payment provider, the merchant can deliver the items with confidence of the consumer's ability to pay for such services and/or goods without maintaining financial

> information about the consumer (e.g., credit card numbers, account information, etc.). In addition, because **the payment provider can validate the authenticity of the payment token as coming from the consumer**, the payment provider can confidently transfer funds to the merchant; thus completing the three-way secure commercial transaction.

Id. at [0042] (emphasis added).

> The identity token may include an electronic signature from the identity provider 120 certifying that the identity credentials are correct. In this way, a merchant and/or payment provider may rely on a disinterested third party (i.e., an identity provider), rather than the representations of an arbitrary end-user. The identity token may be encrypted before being transmitted over the network and decrypted when received by the desired network device (e.g., merchant, payment provider, etc., as discussed in further detail below), to protect against eavesdroppers on the network. **In other embodiments, the payment token is merely a certification of the end-user's identity without accompanying identity information.**

Id. at [0056] (emphasis added).

For reasons described above, the broadest reasonable interpretation of the term "unauthorized service client" should at least include "a service client that is restricted from knowledge sufficient to make ordinary full use of the secured resource outside of the framework of the authentication system." *See*, Section III.D(i). One example provided in the '079 patent specification of restricting a

service client "from sufficient knowledge to make ordinary full use of the secured resource outside" is by not providing the service provider with access to "the common identifier for the secured resource, e.g. the account number for a credit card or financial deposit account." *'079 Patent* (EX1001), at 8:4-10; *see also, id.* at 10:29-36.

Johnson teaches the merchant is an unauthorized service client in that the merchant is restricted from knowledge sufficient to make ordinary full use of the billing account outside of the framework of the authentication system. In particular, *Johnson* teaches that merchants are never granted access to the purchasers' account information:

> Still other embodiments allow for a three-way secure commercial transaction between a merchant, consumer, and payment provide[r] in such a way that **sensitive billing account information is opaque to the merchant or third parties**. In such an embodiment, payment tokens are passed via the consumer between the merchant and payment provider. Such payment tokens are encrypted or signed in such a way that **the merchant and others do not control or obtain any sensitive account information for the consumer**.

Johnson (EX1004), at [0014] (emphasis added).

> Although such payment tokens uniquely identify the authorization of payment for the services and/or goods, **sensitive information about the billing account for the**

> **consumer is either not included within the token or otherwise encrypted so as to be invisible to the merchant. Accordingly, the consumer's sensitive information is opaque to the merchant**, thereby allowing the consumer to confidently purchase items from the merchant even when no trusted relationship exists between them.

Id. at [0042] (emphasis added); *see also, id.* at Abstract, [0067], [0033]–[0037]. Additionally, possessing a payment token does not give a merchant unfettered access to the purchaser's account after the transaction has been completed. Rather, Johnson teaches that each payment token may only be used for a single transaction. *Id.* at [0069], [0072], [0074], [0089]. Thus, after a transaction is complete, the merchant is unauthorized to access the purchaser's accounts without performing the three-party transaction protocol again.

[1(a)] a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource;

In *Johnson*, when a purchaser 110 wishes to buy a good or service from a merchant, the merchant provides billing information to the purchaser along with a request for a payment token. *Id.* at [0059]–[0060], [0089]. As discussed above, the payment token allows the merchant to access funds in the purchaser's account without giving the merchant the purchaser's confidential account information. *Id.* at [0042].

The billing information provided by the merchant includes information such as the cost of the item to be purchased and merchant information, for example:

> Similar to above, local computing device (which can be a handheld portable device as described below in a local retail transaction, a personal computer in an online transaction, or other similar device as described herein) desires various services and/or goods offered by merchant(s) 905. . . . **Such billing information may include, but is not limited to, cost of the merchandise and/or services, detailed description of the commercial transaction, merchant 905 specific information, federation payment information, type of transaction (e.g., single payment, subscription, etc.), or other types of billing information.** The bill information 910 may also include other information such as merchant constraints and payment options as described in greater detail below.

Id. at [0089] (emphasis added).

After receiving the billing information from the merchant, the purchaser generates a request for a payment token from the payment provider. *Id.* at [0060], [0090], Figs. 3, 9. The request for the payment token includes the billing information 910 provided by the merchant in addition to the purchaser's identity token or other identification information. *Id.* at [0090] ("the billing information 910 can be part of the payment token request 980"), [0091], [0093]; Fig. 9. As

shown in the figure below, the purchaser sends the payment token request to the payment provider in step 315:

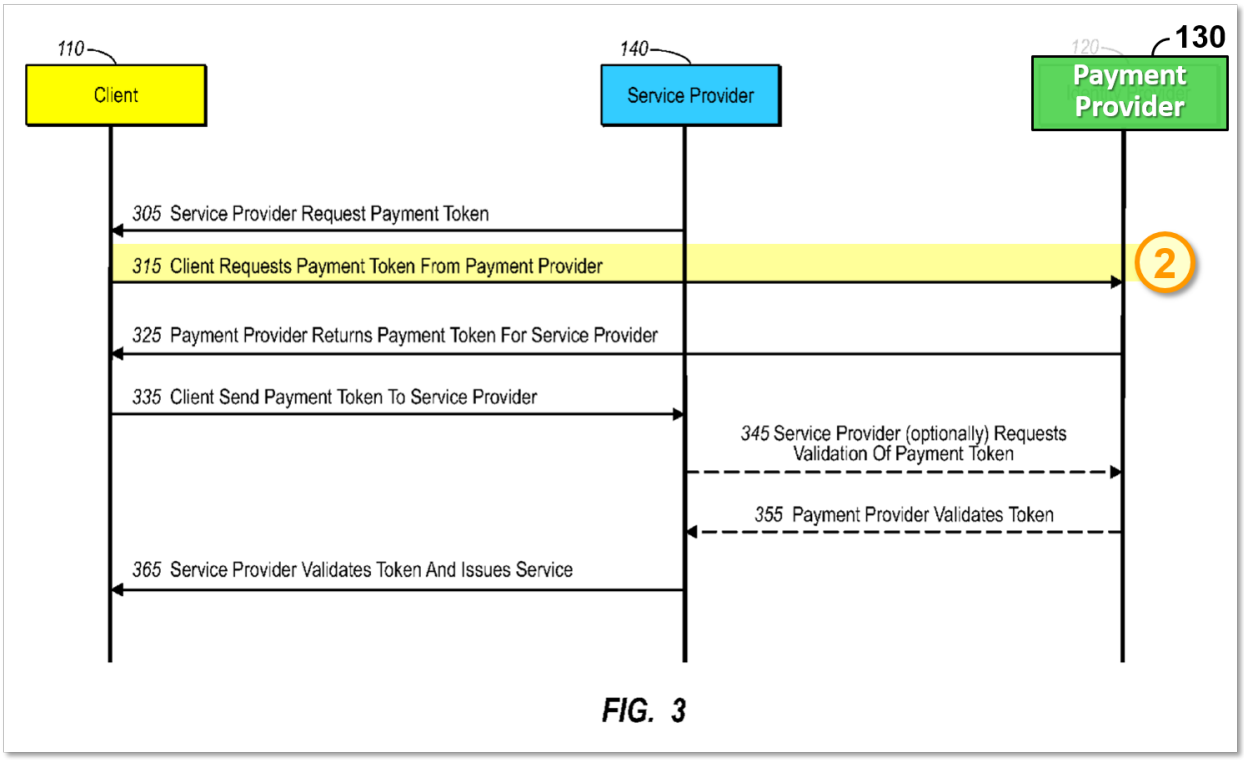


FIG. 3

Id. at Fig. 3 (annotated).

> The end-user computer 110 may solicit a payment token from a payment provider 130 (step 315) by transmitting the identity token to payment provider 130. Alternatively, the end-user may request a payment token by logging onto the payment provider 130 in a manner similar to that discussed in connection with the identity provider 120 . . . . In addition, the end-user may send information about the purchase, such as the price and nature of the purchase so that the payment provider can verify that the end-user is capable of paying.

Id. at [0060]; *see also, id.* at [0089].

The payment token request 980, which is sent in step 315, constitutes the claimed "request for access by an unauthorized service client to said secured resource" that is received from a requester purporting to be an authorized user of a secured resource.

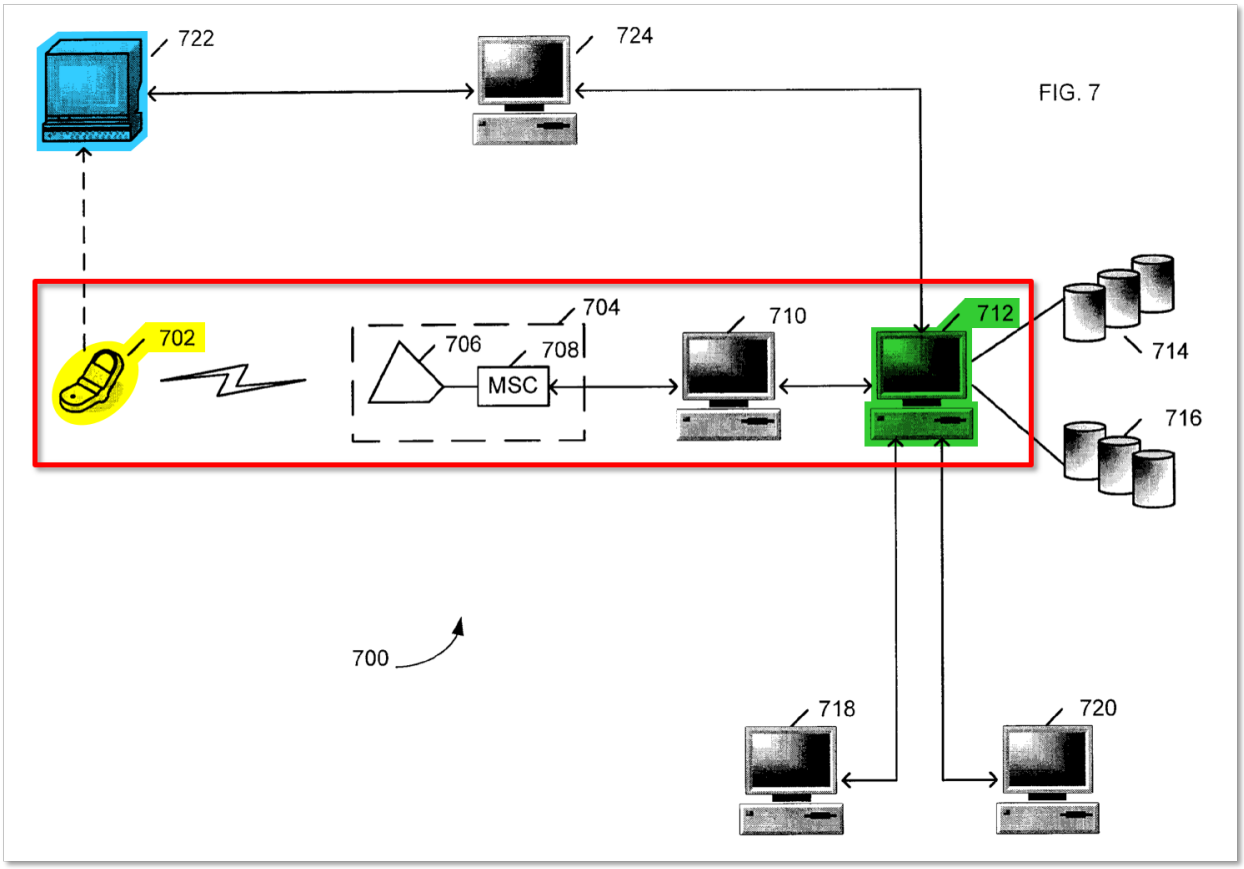
Johnson generally teaches that each party (e.g., purchaser, merchant, payment provider) corresponds to a "network entity" each of which "may have a presence on a network via one or multiple network nodes. For example, multiple networked devices may operate under the auspices of a single network entity, such as an identity provider utilizing multiple servers to conduct online business . . . ." *Id.* at [0040]. *Johnson* also teaches that any networked device used with the system, including the payment provider's device, may be a server:

> The network 105 may have any number of devices connected to it and may be a trusted (e.g., intranet) or an untrusted network (e.g., LAN/WAN, Internet, etc.), or a combination of both. **The computers connected to the network may be any type of device including**, but not limited to, one or any combination of a mobile phone, a desktop computer, a tablet personal computer, **a server**, workstation, etc.

Id. at [0048] (emphasis added).

Johnson does not expressly disclose that an intermediate messaging gateway receives the purchaser's request for a payment token prior to receipt of the request by the payment provider server. However, *Stambaugh* teaches a system utilizing a

similar three-party tokenization protocol where a message authority (710) receives a request for a transaction number from a user via text message, e-mail, or voice message. *Stambaugh* (EX1005), at 2:18-35, 3:53-65, 6:25-31, 6:50-7:2, 8:42-9:3. After receiving the request, the message authority (710) sends the request to a payment authority 712, which generates the transaction number:



Id. at Fig. 7 (annotated).

> First, in step 402, the message authority can receive a message that includes the PIN. As explained above, this message can comprise a text message sent via the SMS system; however, in other embodiments, the message can be sent via the Mobile

> Message Service (MMS) system, via mobile e-mail, or even via voice message, e.g., using voice recognition technology. Once the message is received the payment authority can extract the mobile communication device identifier in step 404 . . . When the message is sent by the user in step 302, the message is typically relayed to the payment authority through a message authority.

Id. at 6:50-66; *see also, id.* at Fig. 4.

> Once a user's account is established, the user will have a PIN that they can input into their mobile communication device 702 and send to payment authority 712 in order to receive a transaction code that they can use to complete a payment transaction. **When the user inputs the PIN into device 702, device 702 can transmit the PIN to payment authority 712 via message authority 710.**
>
> Device 702 can send the PIN via a variety of messaging services. For example, in one embodiment, device 702 can send the PIN via a text message such as an SMS message. Further, in certain embodiments a short code can be associated with payment authority 712. These short codes are typically 5 digits. Thus, the user can simply send an SMS message including the PIN to the short code. In such instances, messaging authority 710 will be a SMSC.
>
> Thus, device 702 can generate a message that is sent to the associated communication network 704. It will be understood that communication network 704 will generally comprise a

> plurality of base station 706 interface [sic] with one or more Mobile Switching Centers (MSC) 708. The message can be received by base station 706 and forwarded to MSC 708, **which can be configured to forward the message to message authority 710**. e.g., the associated SMSC. In other embodiments, device 702 can be configured to send the PIN via an MMS message, in which case message authority will be an MMSC. In still other embodiments, device 702 can be configured to send a PIN via a SkyMail message, a short mail message, via e-mail messaging, e.g., using standard protocol such as SMTP over TCP/IP, etc.

Id. at 8:42-9:3.

As discussed above, the term "messaging gateway" must at least include "a device for use in transferring messages between a plurality of communications channels by converting messages between a plurality of message formats." *See*, Section III.D(ii). *Stambaugh*'s message authority is a device that receives messages in a plurality of formats (e.g., text message (SMS/MMS), email, and voice message) over different communication channels and, in certain embodiments, converts them to IP protocol for transfer to the payment authority. *Stambaugh* (EX1005), at 6:64-7:10 (message authority receives request in SMS format and sends message authority IP address and request message to payment authority over network); 9:41-56 (". . . various other components of the system can communicate using . . . networks, including the Internet and World Wide Web. . . .

the various components are configured to communicate using the requisite communication protocols and signal schemes."). As such *Stambaugh's* message authority constitutes a "messaging gateway" within the meaning of the '079 Patent. *Mott Decl.* (EX1007) at ¶¶68, 71-73.

Johnson broadly teaches implementing the system on "any type of network in any type of configuration that interconnects and allows nodes connected to the network to communicate. Nodes or devices may be connected to the network via copper (e.g., Category 5) cable, optical connections, wireless or any combination thereof." *Johnson* (EX1004), at [0048]. *Johnson* further teaches that various computing devices can be used, including "a mobile phone" and "tablet personal computer" as examples, and that "a mobile module," such as "a subscriber identity module (SIM)," as used in mobile devices, can be used in the system for purposes of authenticating a user and/or device. *Id.* at [0048], [0045], [0054], [0121]. As such, it would have been obvious to a PHOSITA to implement *Johnson* on networks supporting text messaging, emails, and voice to allow end user mobile devices to send payment token requests as taught by *Stambaugh*. *Mott Decl.* (EX1007), at ¶¶73-77. Well before 2011, the payments industry viewed mobile devices, with their convenience and added security through access to device-based SIM identifiers, as a robust channel for secured payment transactions. *Id*. A skilled artisan, therefore, would have appreciated that allowing the user to submit

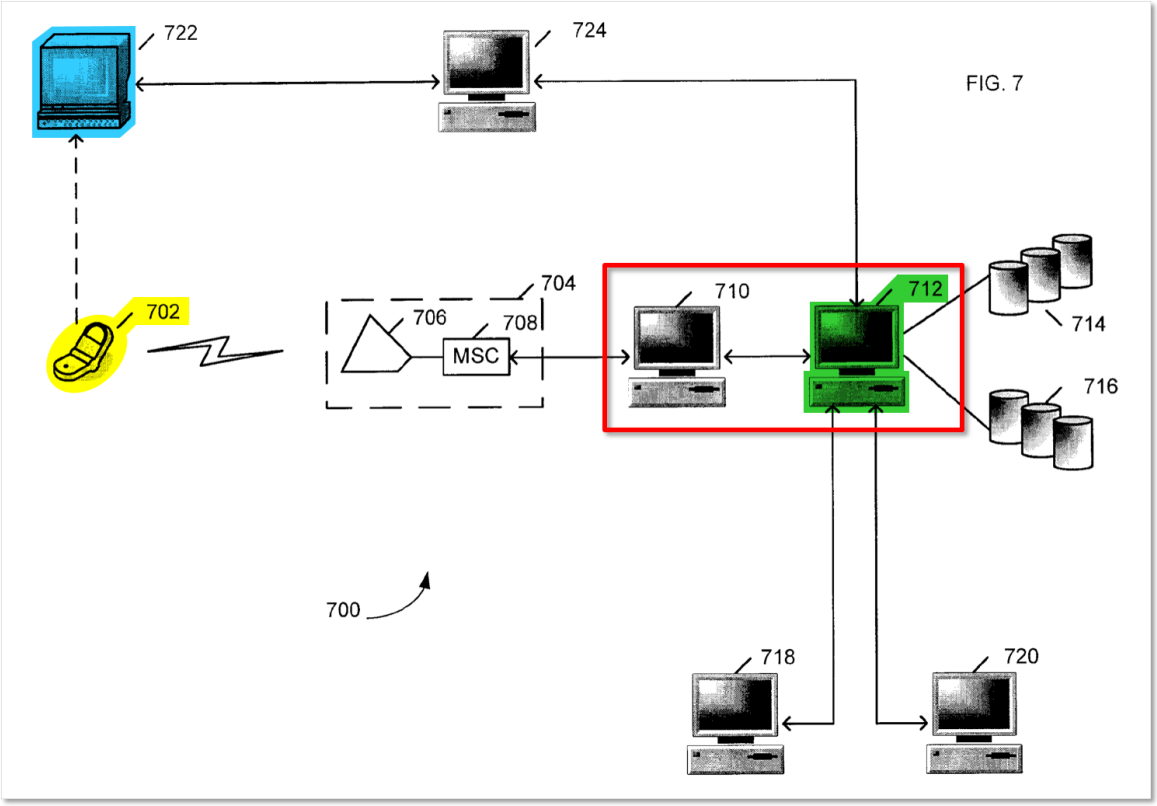
the payment token requests via text message or e-mail, for example, as taught by *Stambaugh*, would have been desirable and an obvious design choice in implementing *Johnson* that would have yielded the predictable result of allowing the user to conveniently submit their payment token requests using their mobile phone or tablet personal computer. *Id*.

It would have further been obvious to include a messaging authority (i.e., messaging gateway), as taught by *Stambaugh*, to receive the payment token request messages via e-mail or text message from the users and convert them to a format compatible for transmission to the payment provider (e.g., via the internet) for processing. *Id*. As opined by Mr. Mott, such gateways have long been (and still are) commonly used when interconnecting one type of network with another type of network in electronic payment systems. *Id*. As such, when enabling *Johnson's* system to be used on a network supporting SMS payment token requests, for example, it would have been obvious to include a message authority to receive the SMS messages from the users and convert them into the communication protocol of the network supported by the payment authority server (e.g., IP network), as taught by *Stambaugh*. *Id*.

[1(b)(i)] a server in secure communication with said messaging gateway,

As described with regard to the limitation above, it would have been obvious to a PHOSITA to include the message authority taught by *Stambaugh* in the system

taught by *Johnson* to receive the request for a payment token from the purchaser. As discussed, *Stambaugh* also teaches that the message authority 710 is in communication with the payment authority 712:



Stambaugh (EX1005), at Fig. 7 (emphasis added); *see also id.* at 6:64-7:10, 8:42-9:3. For reasons described above with regard to limitation 1(a), it would have also been obvious to enable *Johnson's* payment provider server to be in communication with the message authority as taught by *Stambaugh* in order to receive the purchaser requests for payment tokens.

Stambaugh further teaches "secured communication" between the message authority and payment authority by transmitting the message authority's network identifier with the user's request for a transaction number to the payment authority:

> In other words, since the message authority and payment authority are interfaced over a network, the message authority's network identifier, such as the message authority's IP Address or other unique identifier, can be used to ensure that the message is coming from the appropriate message authority in step 408.

Stambaugh (EX1005), at 7:3-10. *Stambaugh* also teaches that "message authority 710 can be configured to provide a digital certificate with the message that can be used by payment authority 712 to authenticate the validity of the message." *Id*. at 9:8-15.

The '079 specification does not include any disclosure regarding establishing "secure communication" between the messaging gateway and the server. The '079 specification generically describes establishing "secure communication" between other system components, but does not provide any details as to how the "secure communications" are to be established. EX1001 at 6:32-37, 10:4-8 (describing "secure communication" between service provider and outside resource providers), 11:36-41 (describing "secured communication" between service client 33 and service provider 36).

As opined by Mr. Mott, identity-based security was (and still is) one well-known way to establish security in communications networks. *Mott Decl.* (EX1007), at ¶78. *Stambaugh's* teaching of transmitting the messaging authority identifier, such as its IP address or digital certificate, to the payment authority establishes a "secure communication." *Id*.

To the extent *Stambaugh's* teaching of using a message authority identifier to secure the communication between it and the payment authority is deemed insufficient, *Johnson* also teaches establishing "secure communication" including, for example, encryption or signing provided by transport level security (TLS), between the network entities, including between the payment provider and the commercial transaction subsystem 965 on the user's local computing device 920:

> Also shown in FIG. 9, and similar to the three-way secure commercial transaction described above, the trust boundary 906 also indicates **a secure communication between the payment provider and the trusted commercial transaction subsystem 965**. Accordingly, the subsystem 965 authenticates to the payment provider(s) 990 in any one of numerous ways described herein, allowing for **secure communication** therewith.

Johnson (EX1004), at [0089] (emphasis added).

> This network security level token can then be used in subsequent authentication phases and provides **transport level security to encrypt and/or sign further interactions** between

> a client and an authentication server and/or mobile infrastructure.
>
> FIG. 7A illustrates an independent network 700 configured to issue a network level security token for establishing **a transport level secure communication** between client and an authentication server.

Id. at [0120]–[0121] (emphasis added). By having the commercial transactions software on each computer, various encryption techniques may be used during transmission of information from one computer to another. *Id.* at [0081]; *see also, id.* at [0045] (describing use of "secure protocols" for "secure communication"); *see also Mott Decl.* (EX1007), at ¶79.

When including a message authority in the system taught by *Johnson*, it would have also been obvious to implement secure communications, including the identity-based security taught by *Stambaugh* and/or the encryption and/or signing using transport level security taught by *Johnson*, between the message authority and the payment provider server. *Mott Decl.* (EX1007), at ¶80. A skilled artisan would have appreciated that applying the well-known communication security methods taught by *Stambaugh* and *Johnson* would achieve the desirable and predictable result of securing communications between the payment provider server and messaging authority, which would further reduce the possibility of malicious parties interfering with the system. *Id*. This would further benefit *Johnson's* goal of reducing the possibility of "security breaches resulting in loss of

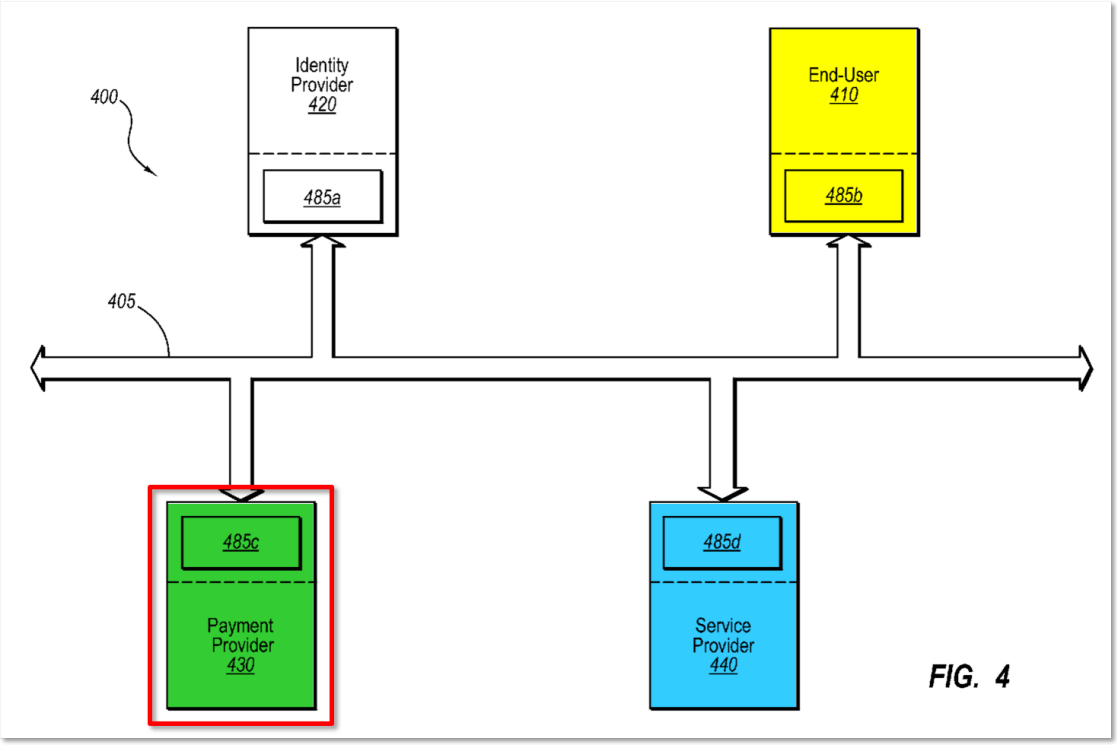
personal, financial, and/or other confidential information," and, indeed, such methods had effectively become mandatory due to their demand in the electronic payments market well before 2011. *Johnson* (EX1004), at [0010]; *see also Mott Decl.* (EX1007), at ¶80.

[1(b)(ii)] said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said key string being adapted to provide a basis for authenticating the identity of said requester;

Johnson teaches a payment provider, which *Johnson* teaches may be a server, having software 485c (i.e., "a second set of instructions embodied in a computer readable medium"):

> The network 105 may have any number of devices connected to it and may be a trusted (e.g., intranet) or an untrusted network (e.g., LAN/WAN, Internet, etc.), or a combination of both. **The computers connected to the network may be any type of device including**, but not limited to, one or any combination of a mobile phone, a desktop computer, a tablet personal computer, a **server**, workstation, etc.

Johnson (EX1004), at [0048] (emphasis added).



Id. at Fig. 4 (annotated).

Johnson's payment provider server software is operable to receive the request for a payment token and generate the payment token:

> The local installation of the **commercial transaction software 485c installed on payment provider 430** can receive the identity token and **generate a payment token** verifying an ability of the end-user to pay (e.g., the payment token) for the online transaction.

Id. at [0079] (emphasis added); *see also, id.* at [0078], [0061]; Fig. 3.

After the payment provider server determines the payment token, it is transmitted back to the purchaser (step 325):

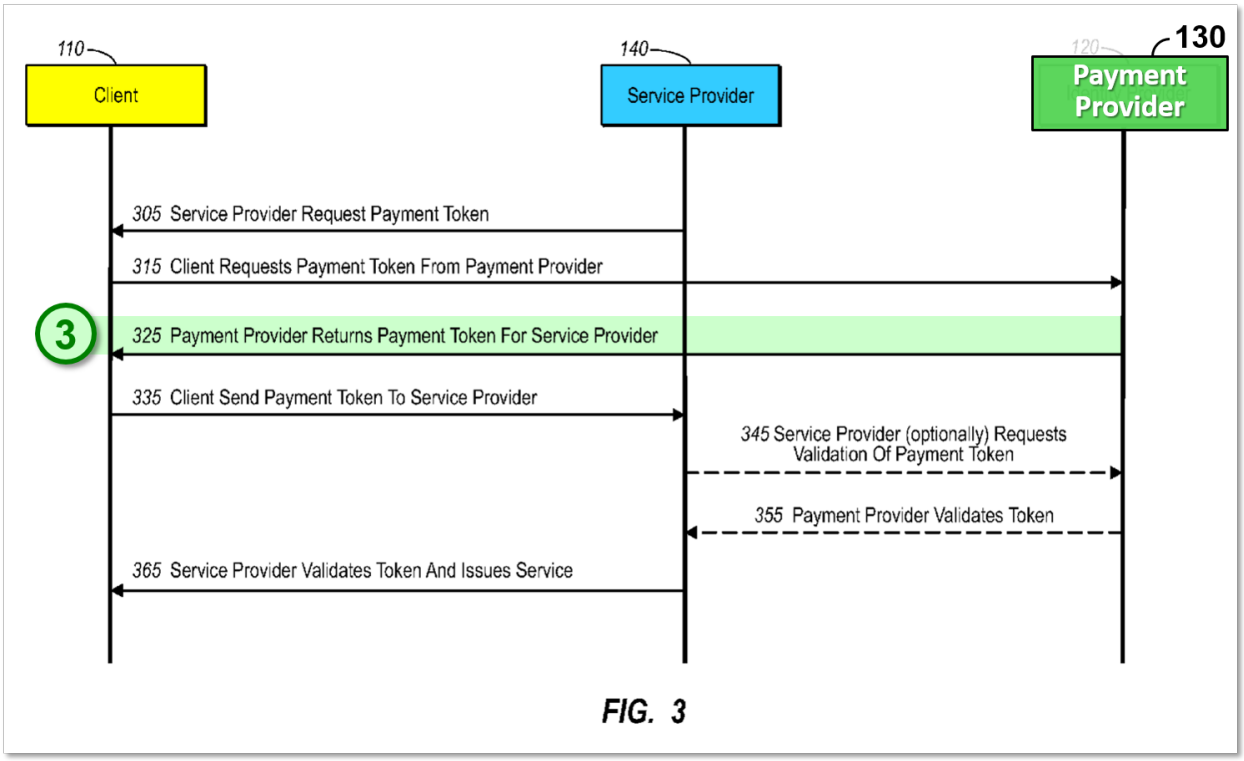


FIG. 3

Id. at Fig. 3 (annotated).

> Payment provider 130 processes the identity token (or other provided identifier) to locate information about the end-user. For example, the payment provider 130 may access a database of payment information based on the identity credentials transmitted with the identity token. Payment provider 130 may determine what payment capabilities and options the identified end-user has available. The payment provider 130 may then verify that the end-user has the ability to pay, and in response generate and transmit a payment token to the end-user computer 110 (step 325).

Id. at [0061]. And *Johnson* teaches that the payment provider may be a financial institution, such as a credit card company or a bank, where the user has an account:

> For example, the dialog box may list payment providers 530 a, 530b and 530c, which may include a credit card company, a bank offering electronic debit services, or a private third party offering financial services, respectively.

Id. at [0099]; *see also, id.* at [0040], [0054]. As such, the payment token is known to both the purchaser and the secured resource.

The payment token provides a basis for authenticating the identity of the purchaser:

> Further, because the merchant can validate the payment token directly with the payment provider, the merchant can deliver the items with confidence of the consumer's ability to pay for such services and/or goods without maintaining financial information about the consumer (e.g., credit card numbers, account information, etc.). In addition, because **the payment provider can validate the authenticity of the payment token as coming from the consumer**, the payment provider can confidently transfer funds to the merchant; thus completing the three-way secure commercial transaction.

Id. at [0042] (emphasis added).

> The identity token may include an electronic signature from the identity provider 120 certifying that the identity credentials are correct. In this way, a merchant and/or payment provider may rely on a disinterested third party (i.e., an identity provider), rather than the representations of an arbitrary end-user. The identity token may be encrypted before being transmitted over

> the network and decrypted when received by the desired network device (e.g., merchant, payment provider, etc., as discussed in further detail below), to protect against eavesdroppers on the network. **In other embodiments, the payment token is merely a certification of the end-user's identity without accompanying identity information.**

Id. at [0056] (emphasis added).

For reasons discussed above, the term "key string" should at least include "an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user 34 and a format that may be recognized by software or hardware that may be used to provide a basis for authenticating the identity of the requester." *See*, Section III.D(iii). While it is clear from *Johnson's* disclosure that the payment token may, at a minimum, be recognized by hardware or software and payment tokens were well known as being strings of symbols, such as alphanumeric characters,[2] *Johnson* nonetheless does not expressly disclose whether the payment token is in a format that may be perceived by the purchaser. *Stambaugh*, however, expressly teaches a similar transaction number, which is generated by a payment authority upon request from a purchaser and which is perceivable by a human and hardware or software. Specifically, *Stambaugh* teaches that the transaction number is a variable length digit code (i.e., an ordered

[2] *Mott Decl.* (EX1007), at ¶81.

sequence) comprising numbers or alphanumeric data that can be displayed on a user's mobile communication device:

> **The transaction code can comprise any data or information that can be displayed on a users, mobile communication device** and that can be input into the POS systems of participating merchants. In certain embodiments, for example, **the transaction code is a 4, 8, etc., digit code comprising purely numbers or alphanumeric data**. As explained below, the length of the code can be variable in certain embodiments.
>
> In one specific implementation, the code is a 4 digit numerical code. Accordingly, once the user is authenticated, the payment authority can be configured to transmit a 4 digit numerical code back to the user's mobile communication device. The device can then display the code to the user so that the user can provide the code to the merchant.

Stambaugh (EX1005), at 7:15-27 (emphasis added). Thus, *Stambaugh* teaches a key string may be both recognized by hardware/software and perceived by an end-user.

It would have been obvious to a PHOSITA for the payment token taught by *Johnson* to be an ordered sequence of numbers or alphanumeric data as taught by *Stambaugh*. *Mott Decl.* (EX1007), at ¶¶81-83. A skilled artisan would have readily appreciated that tokens, including specifically payment tokens, were most commonly ordered sequences of numbers and/or alphanumeric data. *Id*. As such,

using an ordered sequence of numbers and/or alphanumeric data would have been the most natural and routine way for a PHOSITA to implement *Johnson's* payment token. *Id*.

Additionally, in the only embodiment disclosed in the '079 Patent specification, the "key string" is "previously established" prior to the initiation of the transaction. *See e.g.*, *'079 Patent* (EX1001), at 6:18-28. Petitioner notes that the plain language of the claim does not include any requirement for the "key string" to be established prior to the initiation of the transaction. Petitioner further notes that it is improper to read a particular embodiment appearing in the written description into a claim if the claim language is broader than the embodiment. *See In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) ("[L]imitations are not to be read into the claims from the specification.").

However, to the extent the Board finds that a "key string" must be established between a user and service provider prior to the initiation of the transaction, *Stambaugh* teaches a transaction code comprising digits generated by the payment authority that are unique to each transaction and pre-established additional digits appended by the user that are known only to the user and payment authority:

> In still anther aspect, the transaction code sent back to the user can include blanks, or X's that are to be filled in with numbers or data known to the user. In other words, if the transaction is,

> e.g., a four-digit number, then the payment authority can transmit two of the numbers and leave two of the numbers blank. The user can then complete the four-digit code using two numbers known to the user. **In addition to knowing the user's PIN, the payment authority will also know the two numbers known to the user.** Accordingly, when the transaction code is then transmitted back to the payment authority via the POS system, **the payment authority will be able to verify the code as a correct code**.

Stambaugh (EX1005), at at 2:61-3:5 (emphasis added).

> In certain embodiments, **the transaction code can actually comprise** certain digits generated by the payment authority and **certain digits known to the user**. **This can allow an additional factor for authentication.** For example, the payment authority can generate (step 412) a 4 digit code comprising two numbers and two blanks. **When the user receives the code (step 304), they can fill in the blanks with two numbers known to the user and the payment authority**. When the payment authority subsequently receives the transaction code from the transaction authority (step 602**), the payment authority will recognize the complete code as a valid code** and approve the transaction.

Id. at 8:19-30 (emphasis added). Thus, *Stambaugh* teaches that the digits known only to the user and the payment authority provide a basis to authenticate the identity of the user and are established prior to the transaction.

It would have been obvious to a PHOSITA to modify *Johnson* to further require the payment authority to store a code known only to the payment authority and the user and further require the user to append the previously established code to the payment token in order to provide an additional factor of authentication as taught by *Stambaugh*. *Mott Decl.* (EX1007), at ¶¶84-85. This would have predictably enhanced the security of *Johnson's* system thereby furthering *Johnson's* goal of reducing fraudulent transactions. *Id.*

[1(c)] a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client;

Johnson teaches a service provider component 140/440, which is a computer used by the merchant to interface with the payment provider server. *Johnson* (EX1004), at [0046], [0061]–[0062], [0078]; Figs. 3–4. *Johnson* teaches that this computer, like all of the computers for each of the network entities, may be a "desktop computer" or "workstation," for example (*id.* at [0048]), and may utilize Microsoft Windows®. *Id.* at [0080]. The service provider computer includes software 485d (i.e., "a third set of instructions embodied in a computer readable medium") that receives input from the merchant (i.e., "unauthorized service client"), including input of the payment token provided to the merchant by the purchaser and input of the billing information corresponding to the transaction:

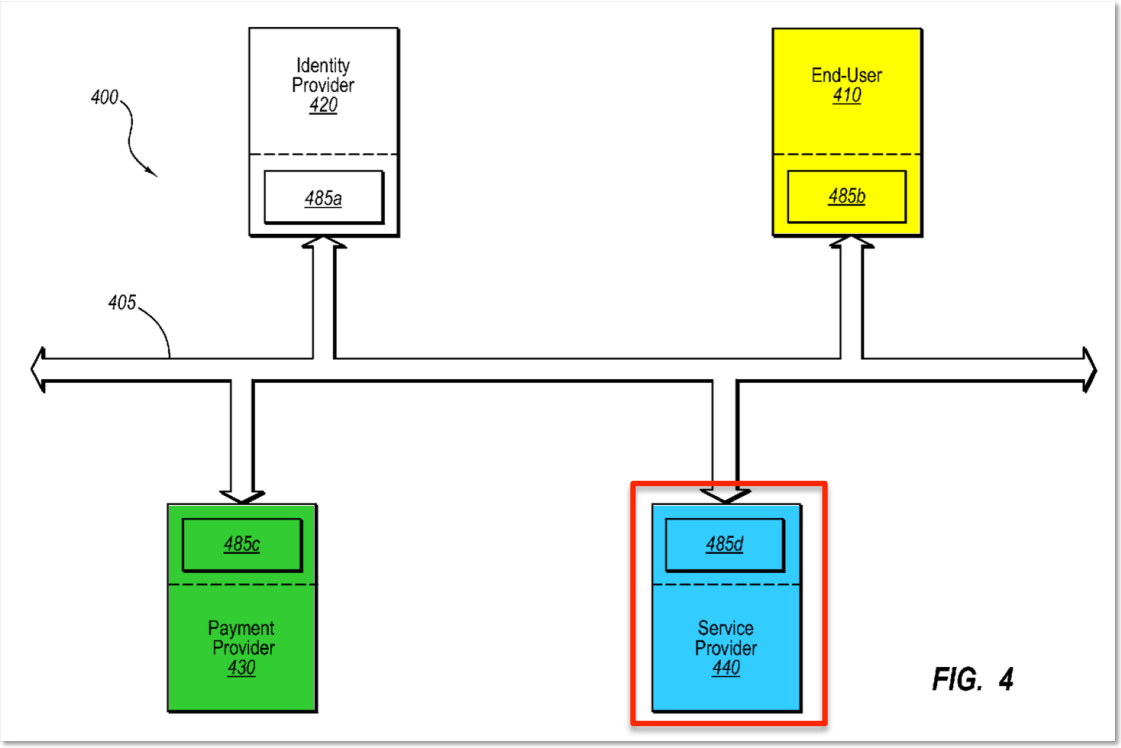


FIG. 4

Id. at Fig. 4 (annotated).

However, in FIG. 4, each of computers in system 400 includes local installations of commercial transactions software 485. In particular, end-user or consumer computer 410, identity provider 420, payment provider 430 and **merchant 440 include commercial transactions software 485a-485d**, respectively. **The commercial transactions software locally installed at each of the computers in the system may be the same, or may be customized for the particular computer in view of which role(s) the computer plays in the transaction** (i.e., whether the computer operates as an end-user node, a merchant node, identity provider node, payment provider node, etc., or some combination of the above). In either case, each

> installation is configured to communicate with installations on other networked computers to perform online transactions. For example, each installation may be configured to communicate with installations on networked computers so as to perform the methods illustrated in FIG. 2 and/or FIG. 3.

Id. at [0078] (emphasis added).

> The end-user computer 110 may then forward the payment token to the merchant 140 (step 335).
>
> The merchant 140 processes the payment token such that the merchant 140 is satisfied that the end-user is able to pay for the goods or services (step 365). For example, the merchant 140 may ask the payment provider 130 to validate the payment token (steps 345, 355) . . . .

Id. at [0061] – [0062].

> For example, one embodiment provides that the billing information 910 can be part of the payment token request 980 (or otherwise delivered in another communication to the payment provider 990) as previously described. As such, the bill information may be used by the payment provider 990 for payment token validation 940. More specifically, the bill information 910 provided from the consumer or local computing device 920 can be compared with the payment token 985 information provided from the merchant 905 in the payment token validation 904. Accordingly, if the bill information 910 for the payment token validation 904 matches the bill information 910 from the token request 980, the

payment provider 990 can be further assured of the authenticity of the payment token 985 and the validity of the merchant.

Id. at [0090].

[1(d)] wherein said second set of instructions is further operable to receive an authentication credential from said unauthorized service client associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requestor; and

Johnson teaches that the payment provider server software (i.e., "said second set of instructions" discussed above for 1(b)(ii)) is operable to receive the payment token (i.e., "an authentication credential") from the merchant (step 345). The payment token was previously provided to the merchant by the purchaser (step 335):

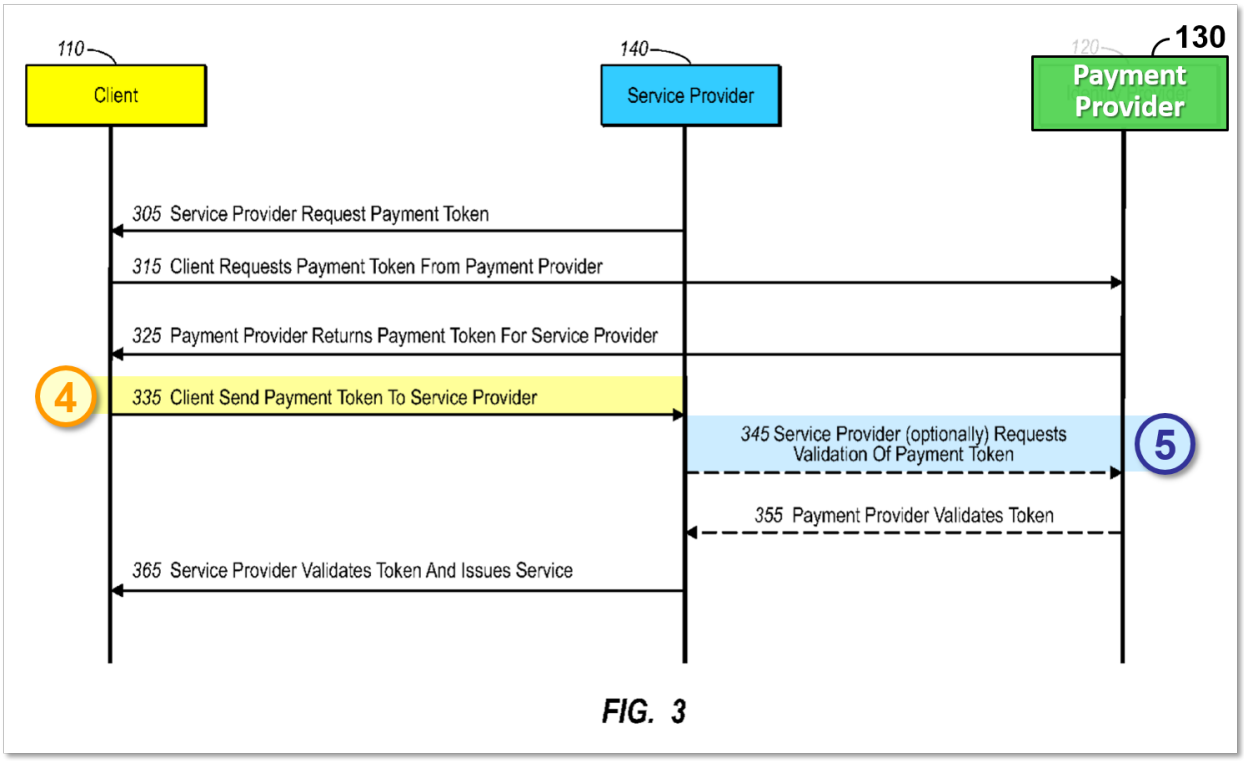


FIG. 3

Id. at Fig. 3 (annotated).

> The end-user computer 110 may then forward the payment token to the merchant 140 (step 335).
>
> The merchant 140 processes the payment token such that the merchant 140 is satisfied that the end-user is able to pay for the goods or services (step 365). For example, the merchant 140 may ask the payment provider 130 to validate the payment token (steps 345, 355) . . . .

Id. at [0061] – [0062]; *see also, id.* at [0089]–[0093] ("payment token validation 904"); Fig. 9.

As discussed above with regard to limitation 1(b)(ii), the only embodiment in the '079 patent specification discloses that the "authentication credential" "simply comprises a previously established key string known to both the service provider 36 and the end user 34." *'079 Patent* (EX1001), at 6:26-28. This authentication credential provided by the end user 34 to the service client 33 is forwarded by the service client 33 to the service provider 36 for validation (just as the payment token in *Johnson* is provided by the purchaser to the merchant and which the merchant then forwards to the payment provider for validation). Again, Petitioner does not believe that the BRI of the claim requires the "authentication credential" to be a "previously established" key string that is established prior to the transaction. However, to the extent the Board finds otherwise, *Stambaugh* teaches a transaction code (i.e., "authentication credential") comprising digits generated by the payment authority that are unique to each transaction as well as

additional digits appended by the user (to fill in "blanks" or "Xs" in the transaction code) that are previously established and known only to the user and payment authority, as discussed above for 1(b)(ii). *Stambaugh* (EX1005), at 2:61-3:5; 8:19-30. For the same reasons described above with regard to limitation 1(b)(ii), it would have been obvious to a PHOSITA to require *Johnson's* payment token to further a include a previously established code known only to the user and payment provider. As taught by *Stambaugh*, it would have also been obvious to require the user to append the additional code to the payment token provided by the payment authority prior to providing the payment token to the merchant. *Mott Decl.* (EX1007), at ¶86. Appending such additional data to tokens was used in the industry prior to 2011, and a PHOSITA would have readily appreciated that providing this additional factor of authentication would have been desirable to further *Johnson*'s goal of reducing fraudulent transactions. *Id*.

[1(e)] wherein said second set of instructions is further operable to evaluate said authentication credential to authenticate the identity of said requester.

Johnson teaches that the payment provider server software (i.e., "said second set of instructions" discussed above for 1(b)(ii)) evaluates the payment token provided by the merchant to "validate the authenticity of the payment token as coming from the consumer:"

> Further, because the merchant can validate the payment token directly with the payment provider, the merchant can deliver the

> items with confidence of the consumer's ability to pay for such services and/or goods without maintaining financial information about the consumer (e.g., credit card numbers, account information, etc.). In addition, because **the payment provider can validate the authenticity of the payment token as coming from the consumer**, **the payment provider can confidently transfer funds to the merchant; thus completing the three-way secure commercial transaction**.

Johnson (EX1004), at [0042] (emphasis added).

> The identity token may include an electronic signature from the identity provider 120 certifying that the identity credentials are correct. In this way, a merchant and/or payment provider may rely on a disinterested third party (i.e., an identity provider), rather than the representations of an arbitrary end-user. . . . **In other embodiments, the payment token is merely a certification of the end-user's identity without accompanying identity information.**

Id. at [0056] (emphasis added).

The validation of the payment token by the payment provider is depicted in Step 355:

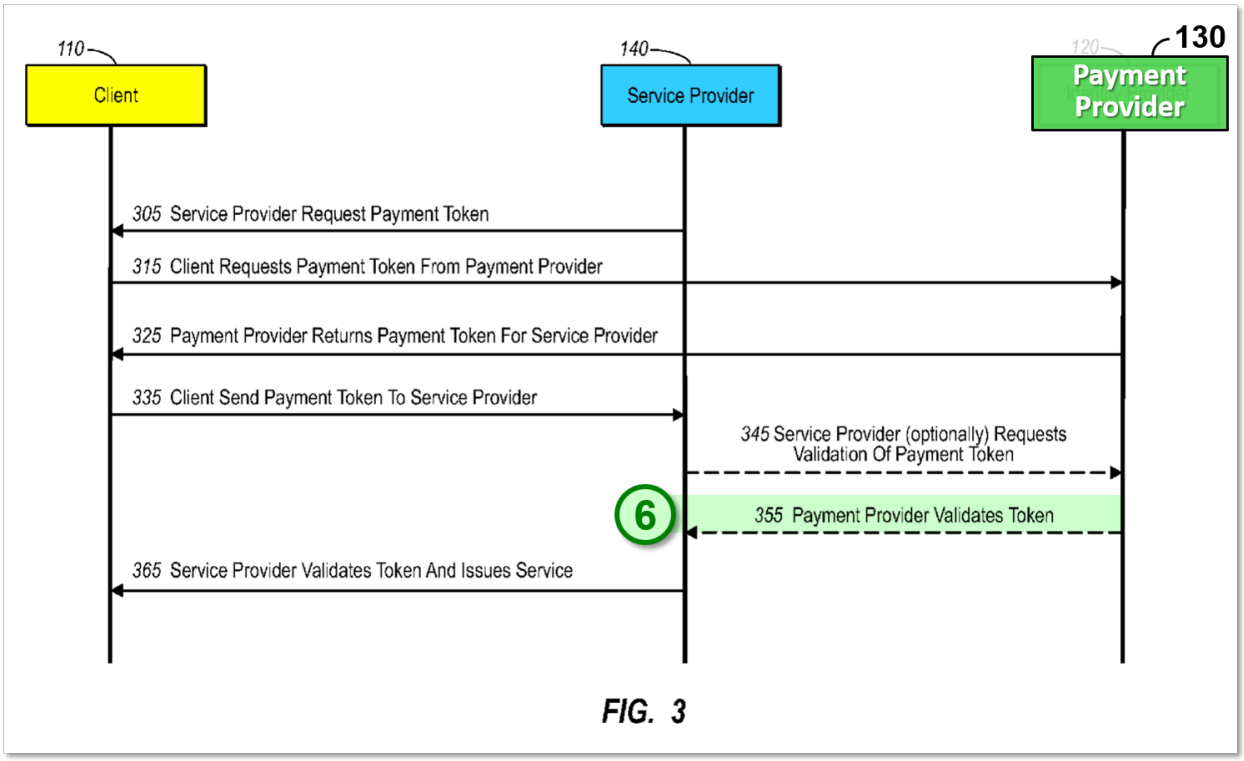


FIG. 3

Id. at Fig. 3 (annotated); [0062]; *see also id*. at [0090]; [0093] ("payment token validation 904"); Fig. 9.

ii. Claim 6

6. The authentication system as recited in claim 1, wherein said second set of instructions includes instructions operable to invalidate said authentication credential based upon passage of time.

As described above, *Johnson* in view of *Stambaugh* teaches Claim 1. In addition, *Johnson* teaches that the payment token may be invalidated upon the passage of a predetermined time limit. The commercial transactions software, which is installed on the payment provider server, processes the time limits associated with the payment tokens:

> Moreover, further security features may be included such as identity tokens and/or **payment tokens that are valid for a limited time period**. For example, an identity token may include a time component that specifies a time after which any component receiving and processing the token should deem it invalid, and not honor the token as verification of identity and/or payment. **The commercial transactions software components may programmatically process any time limits associated with a token**.

Johnson (EX1004), at [0081] (emphasis added).

> FIG. 4 illustrates a networked computer system for handling commercial transactions, in accordance with one embodiment of the present invention. Networked computer system 400 may be similar to computer system 100 illustrated in FIG. 1. However, in FIG. 4, **each of computers in system 400 includes local installations of commercial transactions software 485.** In particular, end-user or consumer computer 410, identity provider 420, **payment provider 430** and merchant 440 **include commercial transactions software 485a-485d**, respectively. The commercial transactions software locally installed at each of the computers in the system may be the same, or may be customized for the particular computer in view of which role(s) the computer plays in the transaction (i.e., whether the computer operates as an end-user node, a merchant node, identity provider node, payment provider node, etc., or some combination of the above).

Id. at [0078] (emphasis added); *see also, id.* at Fig. 4.

iii. Claim 7

7. The authentication system as recited in claim 1, said second set of instructions operable to conduct for the benefit of said unauthorized service client a transaction reliant upon access to said secured resource.

As described above, *Johnson* in view of *Stambaugh* teaches Claim 1. In addition, *Johnson* teaches that the payment provider server software is operable to conduct a financial transaction for the benefit of the merchant. The financial transaction is reliant upon access to the purchaser's billing account:

> For example, one embodiment provides for a three-way secure communication between a merchant, consumer, and payment provider during a commercial transaction for purchasing services and/or goods in either an online or retail environment. As will be discussed in greater detail below, payment tokens are passed from the payment provider to the merchant via the consumer. Such payment tokens offer proof of the consumer's ability to pay for the service and/or goods by allowing the merchant to validate the authenticity of the token directly with the payment provider. Although such payment tokens uniquely identify the authorization of payment for the services and/or goods, sensitive information about the **billing account** for the consumer is either not included within the token or otherwise encrypted so as to be invisible to the merchant. Accordingly, the consumer's sensitive information is opaque to the merchant, thereby allowing the consumer to confidently purchase items

> from the merchant even when no trusted relationship exists between them. Further, because the merchant can validate the payment token directly with the payment provider, the merchant can deliver the items with confidence of the consumer's ability to pay for such services and/or goods without maintaining financial information about the consumer (e.g., credit card numbers, account information, etc.). In addition, because the payment provider can validate the authenticity of the payment token as coming from the consumer, **the payment provider can confidently transfer funds to the merchant**; thus completing the three-way secure commercial transaction.

Johnson (EX1004), at [0042] (emphasis added).

> In addition, because **the payment provider may handle the financial transaction (e.g., handling the credit card, transferring funds, etc.**), the merchant may be relieved of establishing and maintaining the infrastructure necessary to, for example, process credit card numbers or otherwise handle payment procedures and funds transfer. The payment token, in some cases, operates as an assurance that **the payment provider will transmit the designated funds, for example, by wiring the money or enacting an electronic transfer of funds to the merchant**. The payment token may also be an assurance that the payment will be made by non-electronic means such as a promise to issue to the merchant a check or other negotiable instrument.

Id. at [0066] (emphasis added).

iv. Claim 9

9. The authentication system as recited in claim 7, wherein said transaction comprises providing a financial benefit.

As described above, *Johnson* in view of *Stambaugh* teaches Claim 7. As described above with regard to Claim 7, Johnson teaches a transaction comprising providing a transfer of funds to the merchant (i.e., "a financial benefit"). *See Johnson* applied to Claim 7.

v. Claim 11

11. A method for authenticating the identity of a requester of access to a secured resource, said method for authenticating comprising the steps of:

Johnson teaches "networked transaction systems and methods for conducting online transactions." *Johnson* (EX1004), at [0002]. *Johnson's* method includes authenticating the identity of a purchaser requesting access to a billing account. *See Johnson* applied to Claim 1 Preamble.

11[a] receiving at a messaging gateway having a first set of instructions embodied in a computer readable medium, said first set of instructions operable to receive from a requester purporting to be an authorized user of a secured resource, a request for access by an unauthorized service client to a secured resource from a requester purporting to be an authorized user of said secured resource;

See Johnson in view of *Stambaugh* applied to Claim 1(a).

11[b] determining a key string with a server in secure communication with said messaging gateway, said server having a second set of instructions embodied in a computer readable medium operable to determine a key string known to both said secured resource and the authorized user said requestor purports to be, said

key string being adapted to provide a basis for authenticating the identity of said requester;

See Johnson in view of *Stambaugh* applied to Claims 1(b)(i) and 1(b)(ii).

11[c] a service user interface in communication with said server, said service user interface having a third set of instructions embodied in a computer readable medium operable to receive input from said unauthorized service client;

See Johnson in view of *Stambaugh* applied to Claim 1(c).

11[d] wherein said second set of instructions is further operable to receive from said unauthorized service client an authentication credential associated with said request for access, said authentication credential having been provided to said unauthorized service client by said requestor; and

See Johnson in view of *Stambaugh* applied to Claim 1(d).

11[e] wherein said second set of instructions is further operable for evaluating said authentication credential to authenticate the identity of said requester.

See Johnson in view of *Stambaugh* applied to Claim 1(e).

vi. Claim 16

16. The method for authenticating the identity of a requester of access to a secured resource as recited in claim 11, said method for authenticating further comprising the step of determining based upon passage of time whether said authentication credential should be deemed invalid.

As described above, *Johnson* in view of Stambaugh teaches Claim 11. In addition, *Johnson* teaches this limitation. *See, Johnson* applied to Claim 6.

vii. Claim 17

17. The method for authenticating the identity of a requester of access to a secured resource as recited in claim 11, said method for authenticating further comprising the step of conducting for the benefit of said unauthorized service client a transaction reliant upon access to said secured resource.

As described above, *Johnson* in view of *Stambaugh* teaches Claim 11. In addition, *Johnson* teaches this limitation. *See, Johnson* applied to Claim 7.

viii. Claim 19

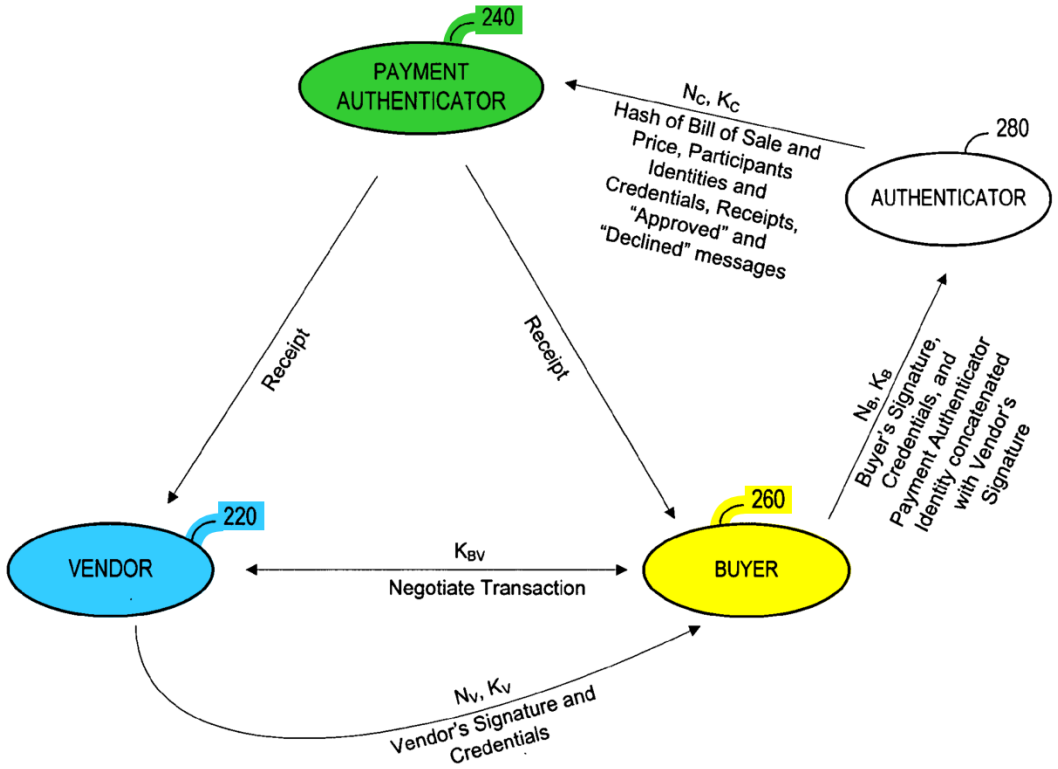
19. The method for authenticating the identity of a requester of access to a secured resource as recited in claim 17, wherein said transaction comprises providing a financial benefit.

As described above, *Johnson* in view of *Stambaugh* teaches Claim 17. In addition, *Johnson* teaches this limitation. *See,* Johnson applied to Claim 9.

B. Ground 2: *Johnson* in view of *Stambaugh* in Further View of *Sellars* Renders Claims 1, 3, 6-9, 11, 13, and 16-19 Obvious

U.S. Patent Application Publication 2006/0173794 to Sellars et al. ("*Sellars*") was published on August 3, 2006 and therefore qualifies as prior art with regard to the '079 Patent under 35 U.S.C. § 102(b) (pre-AIA). *See, Sellars* (EX1006). *Sellars* teaches protocols for performing secure electronic transactions that are similar to those taught by the '079 patent, *Johnson*, and *Stambaugh*. In one embodiment, a buyer 260, which *Sellars* also refers to as "Bob," wishes to electronically purchase a good or service from a vendor 220, which *Sellars* also refers to as "Vera." *Id.* at [0229]–[0230]. Like the '079 patent, *Johnson*, and *Stambaugh*, *Sellars* also teaches that the vendor never has access to the buyer's confidential account information. *Id.* at [0231]-[0232]. A payment authenticator 240, which *Sellars* also refers to as "Carol," "is an entity, such as a credit card company or financial institution, which holds accounts that can be used to finance

transactions (in terms of money or other payment forms or mechanisms)." *Id.* at [0225]; *see also, id.* at [0228]. The buyer, vendor, and payment authenticator are shown, for example, in the below annotated version of Fig. 19:



Id. at Fig. 19 (annotated).

As discussed above, the '079 patent relates to "security protocols for use in securing and/or restricting access to personal other [sic] confidential information, physical locations and the like" and a system and method "whereby the identity of a person, entity, device or the like attempting to gain access to a secured resource may be securely authenticated." *'079 Patent* (EX1001), at 1:6-12. *Sellars* similarly teaches secure electronic commerce protocols for restricting access to confidential account information while authenticating the identities of the parties attempting to

gain access to an account. *Sellars* (EX1006), at [0008]-[0009], [0220]-[0226], [0231]. As such, *Sellars* is in the same field of endeavor and is analogous to the claimed invention of the '079 patent. *See also Mott Decl.* (Ex. 1007), at ¶¶87-88.

The '079 patent seeks to solve problems associated with "the age old process of providing a privately held password, personal identification number or the like in attempting to gain access to the secured resource." *'079 Patent* (EX1001), at 1:29-34. In particular, '079 patent seeks to prevent interception of this sensitive information by an attacker. *Id.* at 1:34-38. *Sellars* also seeks to solve problems associated with electronic commerce transaction protocols where a buyer's "confidential information (e.g., a credit card number, account number, and the like) is communicated from the buyer to the seller." *Sellars* (EX1006), at [0008]. In particular, *Sellars* seeks to solve problems associated with the fact that "once the credit card or confidential information is provided to the seller, the seller has the information indefinitely. There have been instances where the security of that information has been compromised. Such security compromises pose several problems, including consumer wariness of electronic transactions." *Id.* at [0009]. Therefore, *Sellars* is directly related to the problem faced by the inventor '079 patent. As such, *Sellars* is reasonably pertinent to the problem faced by the inventor of the '079 patent and is therefore analogous to the claimed invention of the '079 patent. *See also Mott Decl.* (Ex. 1007), at ¶¶87-88.

i. Claim 3

3. The authentication system as recited in claim 1 wherein said second set of instructions is further operable to for [sic] determine from among a plurality of secured resources associated with said authorized user the identity of a single secured resource to which said requester requests access.

As described above, *Johnson* in view of *Stambaugh* teaches Claim 1. In addition, *Sellar*s teaches that the payment authenticator 240, Carol, is a credit card company or financial institution holding multiple accounts (i.e., "a plurality of secured resources") for the buyer 260, Bob. When Bob wishes to make a purchase from the vendor 220, Vera, Bob generates credentials for the transaction, which identify the account to be used. The account identification is accomplished by either encrypting the credentials with a hash associated with the desired account or prepending an account identifier to the credentials to identify the desired account. Upon receiving Bob's credentials, Carol is able to determine which of Bob's accounts to use for the transaction based on this identifying information. *Sellars* teaches each of the entities, including the payment authenticator 240, Carol, may be implemented using computer systems such as "servers . . . and other devices that have processors or that are capable of executing programs or sets of instructions." *Sellars* (EX1006), at [0054].

> The payment authenticator 240 is an entity, such as a credit card company or financial institution, which holds accounts that can

> be used to finance transactions (in terms of money or other payment forms or mechanisms).

Id. at [0225].

> As with many descriptions of communication protocols, names are assigned to the various entities (or computer systems associated with those entities) used in the protocol. In one embodiment, Bob (B), Vera (P), and Carol (C) represent various participants in a protocol, and Trent (T) represents a trusted arbiter of communication.

Id. at [0228].

> An exemplary embodiment of the protocol involves the four participants discussed above. The entity Bob ("B") performs the role of the buyer 260, the entity Vera ("V") performs the role of the vendor 220, the entity Carol ("C") performs the role of the payment authenticator 240, and the entity Trent ("T") performs the role of the authenticator 280. The protocol involves Bob purchasing goods from Vera. Bob purchases or pays for the goods using an account held by Carol. Trent arbitrates communication between Bob, Vera, and Carol. Since the proposed protocol relies on a trusted authority, Bob, Vera, and Carol trust Trent.

Id. at [0229].

> Bob can generate credentials (B_{cred}) for each transaction, and Carol (who knows Bob's account number and can generate H(x)) can decrypt the credentials (B_{cred}) to obtain the bill of sale and the corresponding price. In some embodiments, if Carol

> **holds multiple accounts for Bob each having account numbers x_1, x_2, . . . , x_n, Carol generates a hash for each account number.** If one of the hashes can decrypt the credentials (B_{cred}), **Carol knows which account to draw funds from**. Bob can also **prepend an account identifier to the credentials (B_{cred}) to identify a particular account**.

Id. at [0234] (emphasis added).

As discussed above, *Johnson's* payment provider 130 may also be a financial institution or credit card company. *See e.g., Johnson* (EX1004), at [0099]. *Johnson* is silent with regard to whether or not the end-user 110 can hold multiple accounts with the payment provider 130. However, a PHOSITA would appreciate that people commonly hold multiple accounts with a single credit card company or financial institution. *Mott Decl.* (EX1007), at ¶89. For example, it was (and still is) common for people to have credit, checking, and savings accounts at a single bank. *Id*. As such, it would have been obvious to a PHOSITA to enable *Johnson's* payment provider to hold multiple accounts for the end-user as taught by *Sellars*. *Id*.

When enabling *Johnson's* payment provider to hold multiple accounts for the end-user, it would have also been obvious to enable the payment provider to determine which account, from among multiple accounts, the user is requesting for a given transaction using the methods taught by *Sellars*. *Mott Decl.* (EX1007), at ¶90. It was common in the industry well before 2011 to allow end users to choose

an available payment option or payment account. *Id*. A skilled artisan would have appreciated that an identifier, such as that taught by *Sellars*, could easily be incorporated in the payment token request sent from the end-user 110 to the payment provider 130 prior to issuance of a payment token in *Johnson*. *Id*. For example, a skilled artisan would appreciate the request could be encrypted with a hash associated with the desired account as taught by *Sellars* or the request could be prepended with an identifier of the desired account known to the user and payment provider as taught by *Sellars*. *Id*. Such an application of known methods would yield the predictable result of allowing the payment provider to determine which of the end-user's accounts to use with the transaction. *Id*. A skilled artisan would further appreciate that this modification to *Johnso*n could be accomplished without ever revealing any of the end-user's confidential account information to the service provider 140. *Id*. Therefore, the security of *Johnson's* system would be maintained, and the modification would not render the system inoperable for its intended purpose. *Id*.

ii. Claim 8

8. The authentication system as recited in claim 7, said second set of instructions further operable to: generate a receipt for said transaction; and transmit said receipt to said authorized user.

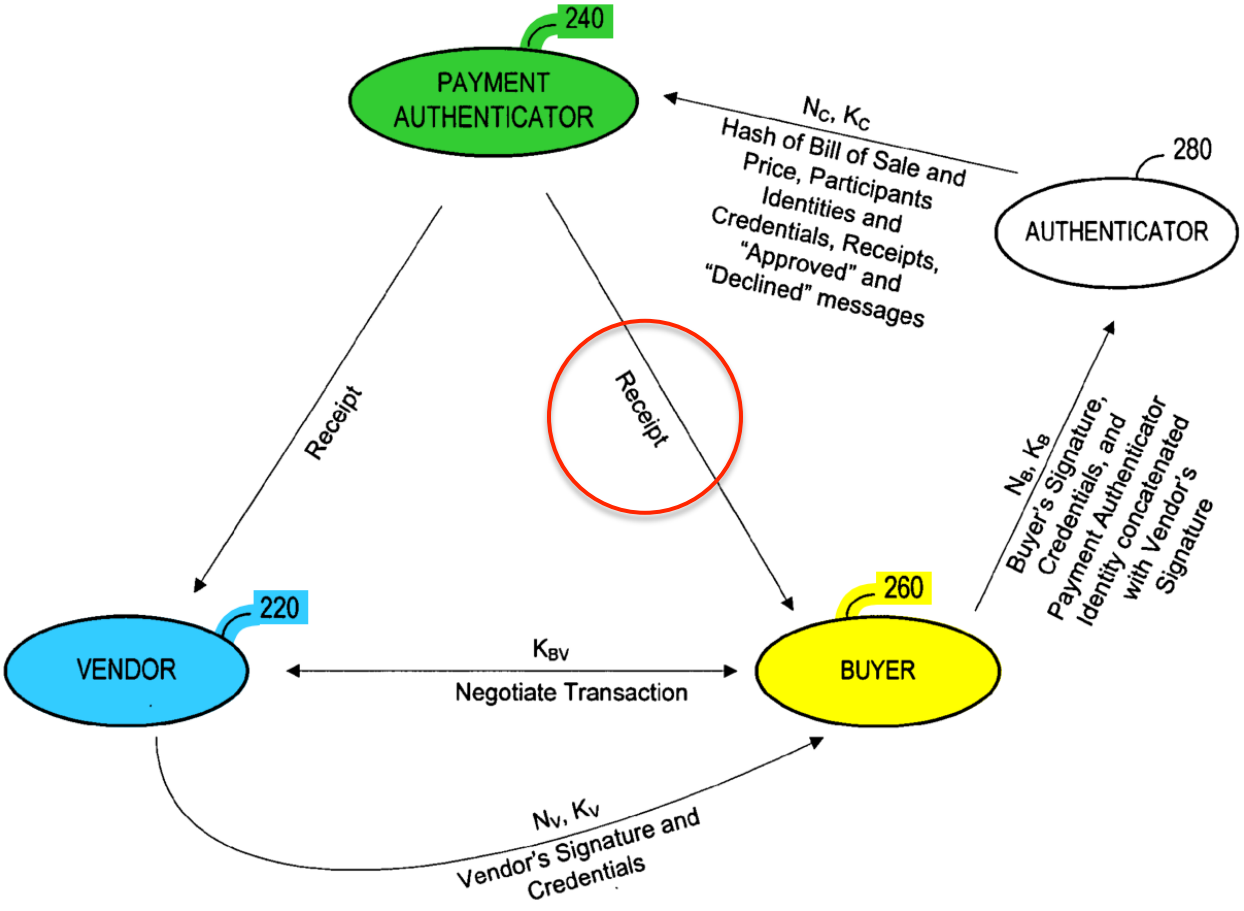
As described above, *Johnson* in view of *Stambaugh* teaches Claim 7. *Johnson* does not expressly teach generation and transmission of a receipt to the

user. And *Stambaugh* does teach generation of and transmission of a "receipt" to the end user for the transaction. *Stambaugh* (EX1005) at 2:45-47; 6:41-44; 7:46-48; 9:34-36. But *Stambaugh* does not appear to expressly teach that the receipt can be generated and transmitted by, specifically, the payment authority (i.e., said second set of instructions on the server). *Sellars*, however, teaches that the payment authenticator 240, Carol, generates a receipt for the transaction between the buyer 260, Bob, and the vendor 220, Vera, and then transmits it to both Bob and Vera:

> Carol receives the payment request and determines whether to approve payment for the bill of sale. In some embodiments, Carol determines whether or not to approve payment by determining if Bob's account (identified by Bcred) contains enough funds to cover the price (P) of the bill of sale. If Bob's account contains enough funds to cover the price, Carol transfers funds from Bob's account to an account of Vera. In some embodiments, Carol can act as an escrow and can hold funds from Bob's account until Vera notifies Carol that goods included in the bill of sale have been shipped and/or provided to Bob. Once the goods have been provided to Bob, Carol can transfer the funds from Bob's account to an account of Vera. **Upon approving payment, Carol can send responses to both Bob and Vera including a receipt,** a new number/key pair, and an approval message.
>
> C→B: E(KB,"Approved")MBRB

C→V: E(KV,"Approved")MVRV

Sellars (EX1006), at [0248] (emphasis added); *see also, id.* at [0228]-[0229], Table 2.



Id. at Fig. 19 (annotated).

Bob is the authorized user because only Bob and Carol know Bob's credentials:

> For the purposes of this example only, assume Bob wishes to purchase goods from Vera. Bob and Vera agree on a bill of sale (S). Bob wishes to pay with funds drawn from an account held with Carol. The account is identified by credentials (B_{cred}). The credentials (B_{cred}) are a secret known or recognizable only to

> Bob, Carol, and Trent. In some embodiments, the credentials (B_{cred}) represent Bob's account number. In other embodiments, the credentials (B_{cred}) are assigned by Trent. Trent does not have to "know" credentials a priori or before hand for the protocol to work. In some embodiments, Trent only forwards credentials to Carol. Furthermore, in some embodiments, Trent cannot obtain the data (such as an account number) included in credentials. This helps increase security of the protocol.
>
> Since the credentials (B_{cred}) are known only to Bob, Trent, and Carol, Trent and Carol can use the credentials (B_{cred}) to verify that Bob created a particular message. Carol may also use the credentials (B_{cred}) to verify Bob's account number. In some embodiments, the credentials (B_{cred}) are constructed from a secret known only to Bob and Carol (such as Bob's account number). The credentials (B_{cred}) can also be constructed from details regarding the current transaction. In some embodiments, the credentials (B_{cred}) are determined as follows:
>
> $B_{cred} = E(H(x), H(S)P)$

Id. at [0230]-[0231].

A PHOSITA would appreciate that it would have been obvious to enable the payment provider 130 taught by *Johnson* to generate a receipt for each transaction as taught by *Sellars*. *Mott Decl.* (EX1007), at ¶¶91-92. Receipts have long been used to record transactions. *Id.* As such, it would have been obvious to enable *Johnson's* payment provider to generate a receipt to document the transaction, as taught by *Sellars*. *Id*. A PHOSITA would have readily appreciated that providing a

receipt to the end-user would have the predictable result of informing the end-user that the transaction has gone through. *Id*. A skilled artisan would also appreciate that such a modification to *Johnson* would have furthered *Johnson's* goal of making the system less susceptible to errors and fraud. *Id*. For example, a receipt would enable the end-user to detect if he or she were overcharged or if there was some other error with the transaction. *Id*.

It would have further been obvious to enable *Johnson's* payment provider 130 to transmit the receipt to the authorized user after approving the transaction as taught by *Sellars*. *Id*. at ¶93. A PHOSITA would appreciate that it would not be useful generate a receipt and then not provide it to the parties involved in the transaction. *Id.* Furthermore, *Johnson* already teaches that the end-user 110 and the payment provider 130 are in bi-directional communication. *Id.* As such, it would have been a simple modification to enable the payment provider to transmit a receipt to the end-user after approving the transaction, as taught by *Sellars*. *Id.*

iii. Claim 13

13. The method for authenticating the identity of a requester of access to a secured resource as recited in claim 11, said method for authenticating further comprising the step of determining from among a plurality of secured resources associated with said authorized user the identity of a single secured resource to which said requester requests access.

As described above, *Johnson* in view of *Stambaugh* teaches Claim 11. *See, Johnson* in view of *Stambaugh* in further view of *Sellars* applied to Claim 3.

iv. Claim 18

18. The method for authenticating the identity of a requester of access to a secured resource as recited in claim 17, said method for authenticating further comprising the steps of: generating a receipt for said transaction; and transmitting said receipt to said authorized user.

As described above, *Johnson* in view of *Stambaugh* teaches Claim 17. *Sellars* teaches this limitation. *See, Sellars* applied to Claim 8.

V. CONCLUSION

For the forgoing reasons, Petitioner respectfully requests *inter partes* review of claims 1, 3, 6–9, 11, 13, and 16–19 of the '079 Patent.

Respectfully submitted,

BY: */s/ Jason R. Mudd*
Jason R. Mudd, Reg. No. 57,700
Eric A. Buresh, Reg. No. 50,394
Jonathan Stroud, Reg. No. 72,518

ATTORNEYS FOR PETITIONER

VI. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)

A. Real Party-In-Interest

The Petitioner is the real party-in-interest. 37 C.F.R. § 42.8(b)(1). No other party exercised control or could exercise control over Petitioner's participation in this proceeding, the filing of this petition, or the conduct of any ensuing trial. In this regard, Petitioner has submitted voluntary discovery. *See* EX1008 (Petitioner's Voluntary Interrogatory Responses).

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), the '079 Patent is presently the subject of the following patent infringement lawsuits:

- *Textile Computer Systems, Inc. v. Forth Worth City Credit Union*, Case No. 2:16-cv-01048 (E.D. Tex.);
- *Textile Computer Systems, Inc. v. Sabine Federal Credit Union*, Case No. 2:16-cv-01047 (E.D. Tex.); and
- *Textile Computer Systems, Inc. v. East Texas Professional Credit Union*, Case No. 2:16-cv-00702 (E.D. Tex.).

C. Lead and Back-Up Counsel

Petitioner provides the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4). Please direct all correspondence regarding this proceeding to lead and back-up counsel at their

respective email addresses: jason.mudd@eriseip.com, eric.buresh@eriseip.com, ptab@eriseip.com, and jonathan@unifiedpatents.com. 37 C.F.R. § 42.8(b)(4).

Lead Counsel	Back-Up Counsel
Jason R. Mudd (Reg. No. 57,700) jason.mudd@eriseip.com ptab@eriseip.com Postal and Hand-Delivery Address: ERISE IP, P.A. 6201 College Blvd., Suite 300 Overland Park, Kansas 66211 Telephone: (913) 777-5600	Eric A. Buresh (Reg. No. 50,394) eric.buresh@eriseip.com ptab@eriseip.com Postal and Hand-Delivery Address: ERISE IP, P.A. 6201 College Blvd., Suite 300 Overland Park, Kansas 66211 Telephone: (913) 777-5600
	Jonathan Stroud (Reg. No. 72,518) jonathan@unifiedpatents.com Postal and Hand-Delivery Address: Unified Patents Inc. 1875 Connecticut Ave. NW, Floor 10 Washington, D.C., 20009 Telephone: (202) 805-8931

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent 8,505,079 B2 to Nandakumar (*'079 Patent*)
Exhibit 1002	File History of U.S. Patent 8,505,079 B2 to Nandakumar (*'079 Patent File History*)
Exhibit 1003	U.S. Patent Application Publication No. 2009/0259588 to Lindsay (*Lindsay*)
Exhibit 1004	U.S. Patent Publication 2006/0235796 A1 to Johnson et al. (*Johnson*)
Exhibit 1005	U.S. Patent 7,657,489 B2 to Stambaugh (*Stambaugh*)
Exhibit 1006	U.S. Patent Application Publication 2006/0173794 A1 to Sellars et al. (*Sellars*)
Exhibit 1007	Declaration of Stephen Craig Mott (*Mott Decl.*)
Exhibit 1008	Petitioner's Voluntary Interrogatory Responses
Exhibit 1009	U.S. Patent 7,140,036 to Bhagavatula et al. (*Bhagavatula*)
Exhibit 1010	U.S. Patent 7,051,002 to Keresman, III et al. (*Keresman*)
Exhibit 1011	FFIEC Authentication Guidance, October 12, 2005
Exhibit 1012	PCI Press Release Regarding Tokenization Guidelines (August 12, 2011)
Exhibit 1013	PCI DSS Tokenization Guidelines (August 2011)
Exhibit 1014	Microsoft Computer Dictionary, 5th Edition, excerpt
Exhibit 1015	U.S. Patent 5,883,810 to Franklin et al. (*Franklin*)
Exhibit 1016	U.S. Patent 7,461,028 to Wronski (*Wronski*)

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 13,987 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: November 21, 2016

BY: */s/ Jason R. Mudd*
Jason R. Mudd, Reg. No. 57,700

ATTORNEY FOR PETITIONER

CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105, the undersigned certifies that on November 21, 2016, a complete and entire copy of this Petition for *Inter Partes* Review including exhibits was provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '079 Patent as listed on PAIR:

Gunn, Lee & Cave, P.C.
300 Convent Street
Suite 1080
San Antonio, TX 78205

BY: */s/ Jason R. Mudd*
Jason R. Mudd, Reg. No. 57,700

ATTORNEY FOR PETITIONER